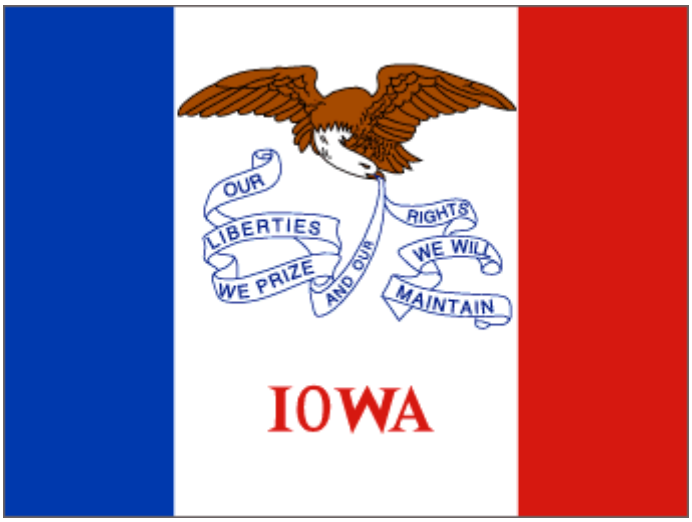
State of Iowa

Criminal Justice Information System Integration Plan



August 26, 2005

1 Executive Summary

The Executive Summary will be an introduction to the document and provide enough material for executive leadership to gain understanding and insight to the strategic plan. The material in this section will present a high-level overview of the artifacts produced in the development of the strategic plan, including descriptions of the current Iowa Criminal Justice Information System (CJIS) environment, the vision of the integrated environment, and the implementation plan necessary to achieve it.

1.1 Project Description

The project description will provide background and foundational information about the CJIS initiative as well as the State of Iowa CJIS Integration Plan project. It is meant to provide the reader with a context of how the CJIS initiative evolved and what it is expected to achieve.

1.1.1 Definition of Criminal Justice Integration

The key to understanding criminal justice information sharing (CJIS) is to address it as an enterprise-wide issue, rather than something that one agency must undertake on its own. SEARCH, the National Consortium of Justice Research and Statistics, defines CJIS as "the ability to share critical information at key decision points throughout the justice enterprise."[1]

In order for CJIS to work in practice, there are several "ground rules" to which participating agencies and the overall effort must adhere. These principles require that:

- Information is captured at the originating point, rather than reconstructed later.
- Information is captured once and reused, rather than re-captured when needed again.
- Integrated systems fulfilling these functions are comprised of, or derived from, the operational systems of the participating agencies; they are not separate from the systems supporting the agencies.
- Justice organizations retain the right to design, operate, and maintain systems to meet their own operational requirements. However, as with any network capability, participants must meet agreed-upon data, communication and security requirements, and standards in order to participate.
- Whenever appropriate, standards will be defined, with user input, in terms of performance requirements and functional capabilities, rather than hardware and software brand names.
- Security and privacy are priorities in the development of integrated justice capabilities and in the determination of standards.

[1] *Integration in the Context of Justice Information Systems: A Common Understanding*, SEARCH, the National Consortium for Justice Research and Statistics, 2004, page 9 (hereinafter *Common Understanding*).

- Integration builds on current infrastructure and incorporates capabilities and functionality of existing information systems, where possible.
- Because of the singular consequences of decision making throughout the justice enterprise, establishing and confirming the positive identity of the record subject is crucial.[2]

1.1.2 Iowa CJIS Overview

In Iowa, the CJIS initiative began in 2001, with the creation of a Memorandum of Understanding (MOU) between the Governor and the Chief Justice of the Supreme Court. It created a CJIS Board that includes the Governor, the Chief Justice of the Iowa Supreme Court, the Director of the Department of Administrative Services or his or her designee, and the State Court Administrator. The duties of the Board are to review recommendations submitted by the Advisory Committee and set policy for the State relating to all aspects of an integrated criminal justice information system, including design, development, funding, implementation, and operation. The Board may adopt or disapprove the recommendations of the Advisory Committee.

The Advisory Committee is the active working group overseeing the CJIS initiative in Iowa. According to the MOU, the Advisory Committee shall be composed of the following members:

- Four representatives of the Judicial Branch appointed by the Chief Justice.
- Four representatives of the Executive Branch appointed by the Governor.
- One representative of each of the following associations: Iowa County Attorney's Association, Iowa State Sheriff's and Deputies Association, Iowa Association of Chiefs of Police and Peace Officers, Iowa League of Cities, and Iowa State Association of County Supervisors. The leadership of each association shall appoint the association's representative.
- Two members of the Iowa Senate, including one Democrat and one Republican, each to be appointed by the leadership of their respective caucus, to serve as ex-officio members.
- Two members of the Iowa House of Representatives, including one Democrat and one Republican, each to be appointed by the leadership of their respective caucus, to serve as ex-officio members.

At its inception, the Advisory Committee was charged with conducting an in-depth examination of the existing criminal justice information systems that exist or are being developed around the state and assess their capabilities from both a technological and a procedural perspective. From this examination, it was charged with making recommendations to the Board regarding policies in the areas of privacy, security,

[2] *Common Understanding*, page 9.

standards, planning, funding, operations, technology, architecture, legislation, and any other issues related to sharing criminal justice information among and between agencies.[3]

To that end, the Advisory Committee undertook a number of activities, including documenting the information exchanges that take place among criminal justice agencies in Iowa, as well as those that occur in the juvenile justice system. These studies documented the current workflow as well as process gaps and places where automation would greatly improve the administration of justice in Iowa.

In 2004, the MOU was amended to require the CJIS Advisory Committee to create a strategic plan to guide CJIS implementation in Iowa. Specifically, the addendum required the CJIS Integration Plan to be based upon interfaces and data transfers, and preserve existing information systems, procedures, and business practices of individual agencies. The MOU further states that the plan "may incorporate the use of a common case management system, procedures, and business practices of individual agencies with similar or common functions. However, CJIS shall not be a single, centralized system, nor is it intended to mandate the elimination or significant modification of individual agency information systems, procedures, and practices."[4]

1.1.3 CJIS Integration Plan Background

On December 13, 2004, the State of Iowa released its Request for Proposals (RFP) for services associated with the creation of its CJIS Integration Plan. The stated objective of the RFP and project is to "develop a specific plan and define appropriate strategies, processes, and technologies necessary to integrate state and local criminal justice information systems and related databases. This project will address the independent and disparate criminal justice information system environment in the State. The outputs of this project will provide the basis for the State to select and implement criminal justice information system integration applications and architectures."[5]

Proposals were due to the State of Iowa on January 28, 2005. The State received responses from three vendors. Upon evaluation of the proposal responses, the State selected the team of MAXIMUS and URL Integration. A contract between MAXIMUS and the State of Iowa was negotiated and executed on April 24, 2005. A contract between MAXIMUS and URL Integration was executed shortly thereafter.

[3] State of Iowa, Memorandum of Understanding: Criminal Justice Information System at http://www.state.ia.us/government/dhr/cjjp/images/pdf/finalCJIS_MOU.pdf (hereinafter MOU).
[4] Addendum to the Memorandum of Understanding: Criminal Justice Information System at http://www.state.ia.us/government/dhr/cjjp/images/pdf/CJIS%20MOU%20Addendum.pdf (hereinafter MOU Addendum).
[5] *State of Iowa Criminal Justice Information System Integration Plan*, page 5 (hereinafter CJIS RFP).

The primary work on the contract began in late April 2005 and extended through August 2005. The final deliverable – the Iowa CJIS Integration Plan – was delivered to the State on August 26, 2005.

1.1.4 CJIS Integration Plan Scope and Objectives

The RFP issued by the State of Iowa included several requirements for the Iowa CJIS Integration Plan. An underlying premise of the RFP was to understand the disparate information systems in use in Iowa and ensure the plan addresses those disparities. It required the final deliverable to map to a five-year implementation timeframe and provide cost estimates that map to each of those years. It required the vendor to demonstrate its review and understanding of the previous studies commissioned by the CJIS Advisory Committee and included a series of important technical requirements around data standards and security. The RFP also required that the plan address specific benefits associated with integration, such as improved decision making and reduced redundant data entry.

The MAXIMUS/URL Team and the CJIS Project Manager created interim deliverables for review and approval by the CJIS Advisory Committee over the course of the five-month project. The MAXIMUS/URL Team presented these deliverables at the monthly CJIS Advisory Committee meetings for comment, review, and payment approval. The interim deliverables include the As-Is Business Assessment, As-Is Technical Assessment, To-Be Environment, Implementation Timelines, and Cost Assessments. Each of these deliverables is a component of the final Integration Plan and comprises the body of this document.

1.2 Project Findings

The Project Findings section will present the high-level "As-Is" and "To-Be" descriptions of the Iowa CJIS environment as well as the summary components of the Integration Plan itself.

1.2.1 Iowa As-Is Environment and Readiness for Integration

An integral part of the implementation plan will be providing a baseline of the current state of the business and technical environments in Iowa that is part of a CJIS solution. This section will provide an executive level description of those two aspects of the CJIS initiative. To gather this information, the MAXIMUS/URL Team employed a variety of information gathering techniques, such as an online survey of local justice practitioners, interviews with individuals who manage large state-level systems, and follow-up phone calls.

1.2.1.1 As-Is Business Environment and Readiness for Integration

The justice business environment in Iowa currently supports automated information sharing among some agencies. For example, there are important state-to-state exchanges that demonstrate Iowa's ability to and interest in exchanging information electronically

between agencies. While most of these exchanges happen via FTP, the protection order exchange between Department of Public Safety (DPS) and the Courts demonstrates significant promise for real-time information sharing. In addition, the interface, while laborious to create, is compliant with strict DPS security regulations.

The State is also conducting local-to-state automated data sharing (but not workflow integration) with its Kaleidoscope and Criminal Justice Information Network (CJIN) efforts. In addition, the TraCS program, which is managed by the Department of Transportation (DOT), is a great example of an automated workflow exchange for local law enforcement to communicate directly with local Courts. The significance of these efforts is that they allow for an entry for local law enforcement agencies with different levels of automation to participate in the broader statewide information sharing effort.

With regard to local level readiness for integration, the survey the MAXIMUS/URL Team developed posed general questions about agency readiness to change their business practices to support justice information sharing. However, when asked questions about specific documents or exchanges, agencies that would benefit from information reported seeing the most value in effort of exchanging information electronically, while those that provided the information or had to data enter it were less certain about whether the exchange at hand would be a useful automated transaction. *This seems to be a common theme among the survey results: in concept, practitioners are supportive of CJIS, but are more interested in changing their business practice to facilitate automation if it makes their job easier; practitioners are less interested if it appears as if the business process change and/or automation would require more work.*

When asked to provide general comments on the usefulness of CJIS in Iowa, participants provided a wide range of opinions. Most who provided commentary agreed that the CJIS concept is necessary in Iowa; one respondent noted that "this is a great initiative. So much of the resources in this area are duplicated between agencies." However, for many respondents, the support was couched in concerns about how the effort would be implemented. There was significant concern about the costs of implementing CJIS, from a funding, staffing, and infrastructure perspective, as well as recognizing the current differences in business practices between large and small agencies in Iowa. One respondent noted:

> *"The main concern I have with standardization is that one-size does not always fit all and the standardized forms are normally prepared to meet the needs of the larger jurisdictions and the smaller jurisdictions are then supposed to accommodate the changes. The other concern I have is that some of these changes will probably require the purchase of additional equipment, software, etc., and you have to be careful about the financial burden this may place on local agencies."*

Another respondent spoke eloquently to the importance of promoting an enterprise-wide view in support of CJIS:

> *"If information sharing is to work, the additional burden for data entry must be shared equally. If the burden falls primarily on one agency with that agency receiving little in benefits, then that agency will be resistant. This has happened in the past with Courts. Clerks of Court believe their data entry duties have been increased to help other agencies but they see little benefit in return to them or the judicial system as a whole for the extra work."*

In addition to these issues around business process change, standardization, and taking an enterprise-wide view of the responsibilities associated with CJIS implementation, there are other common themes that emerged from the survey responses and interviews:

- Most criminal justice practitioners are comfortable that information security can be maintained in an integrated environment.
- Practitioners are confident in their current policies, practices, rules, and statutes around information sharing.
- Participating in automation (e.g., sending information to the CJJP JDW, participation in TraCS) has required groups with disparate forms and business practice to come together and agree on a common approach.
- Current automated exchanges between agencies – whether state-to-state exchanges or local-to-state exchanges – are successful and improve the current business process.
- The goals of automation and information sharing are to improve the business process and make important information readily available to justice practitioners. But there is significant concern about the staffing burden that will be created if a CJIS solution is implemented.

However, as a part of the goals the justice community has set for itself over the last several years, coupled with the findings from the various studies that have been undertaken, the current environment highlights how much work is yet to be accomplished. The MAXIMUS/URL Team made several key observations about the current business environment and readiness for information sharing:

- The State has a very robust Justice Data Warehouse that is limited only by the lack of integration between the feeder agencies/branches.
- The State systems share information with each other, but this is primarily for the purpose of populating individual data warehouses to be used by the agency's/branch's stakeholders alone.
- There are diverse business practices in the justice community at the local level.
- Documents shared between agencies vary from jurisdiction to jurisdiction, but there is movement to standardize some of these forms.
- There are very few transaction-based exchanges. Where there are such exchanges they are successful but are currently held back by the technology employed. In

addition, the successes have not been used as springboards to other similar, but perhaps more challenging, exchanges.

- The State agencies do not use a common data representation, such as numerical identifiers, among their systems.
- The local agencies have disparate systems but share common applications (TraCS) or are moving in that direction (County Attorney Case Management Systems). That said, there is currently significant disparity in the level of automation employed at local agencies.
- The justice leaders and practitioners, for the most part, have expressed a willingness to adjust their systems and practices to accommodate the CJIS initiative, which is seen as for the greater good.

The review of past studies, interviews with the State agency representatives, and the survey results all show the limitations of the current level of integration in Iowa. They also show that Iowa has many of the strengths necessary to build a successful integrated justice information system and cognition of what it will take to move forward.

1.2.1.2 As-Is Technical Environment and Readiness for Integration

At the State level, the Judicial Branch, as represented by the State Court Administrator's office (SCA), the Department of Corrections (DOC), the Department of Public Safety (DPS), the Department of Transportation (DOT), and the Criminal Juvenile Justice Planning division (CJJP) together represent the most significant portion of the foundation for an integrated justice environment in the State of Iowa. Each of those participants currently maintain at least one major information system to handle their internal business processes as well as administer multiple interfaces between themselves and other agencies. They are already exchanging data on a daily basis, and in some cases, a real-time basis. While some legacy technology systems exist within DOT and DPS, each has systems that are moving toward becoming web-enabled or web-based utilizing current RDBMS products for the database layers.

At the local level, there are various system implementations. Such local systems are incident-based and represent the initial data capture environment for the integrated environment. The current implementations are broken down into three major categories: records management systems (RMS) and jail management systems (JMS) for local law enforcement and case management systems (CMS) employed by County Attorney offices. However, CMS, JMS, and RMS systems are not 100% implemented across the counties and municipalities of Iowa. Furthermore, those with systems have systems that vary by vendor, functionality (especially with respect to supporting a service-oriented architecture), and scope. In some instances, the TraCS system is utilized as the de-facto RMS system. A common middle tier allowing these systems to participate in service-oriented architectures is presented later in the Plan recommendations.

1.2.1.3 Network Connectivity

Any statewide, integrated justice effort requires that all local and State participants be interconnected. Fortunately, the Iowa Communications Network (ICN) fiber wide-area network (WAN) has a point-of-presence in each county, private telecommunications companies provide local feeds to the ICN, and each of the above mentioned participants have established use of the ICN for their systems. The ICN is a separate entity, and as such, provides and administers the network usage in cooperation with the SCA, DOC, DPS, DOT, and CJJP via service level agreements. In the case of DOC, a private software vendor, ATG, manages the Department's use of the ICN on their behalf. DPS has the most restrictive network requirements due to its adherence to established NCIC protocols for secured access. The ICN is a strong vehicle for many agencies to participate in the CJIS initiative; however, the ICN is not offered to all local level justice participants, namely, the County Attorneys.

1.2.1.4 Current Security Policies

Justice data by its nature requires a secure environment for information system processing, and these major systems all take this into account by providing secure transmission, user training, and user account management and level of access controls based upon job function. Additionally, these systems all implement their own level of control with respect to network access by either directly or through ICN staff, configuring firewall controls and access control lists. IOWA System users must also adhere to NCIC certification and audit criteria, its own Rules and Regulations, as well as user, location, and terminal identification. A series of security protocols and practices is already established, and any effort to move existing interfaces to transaction-driven data exchanges within the context of a workflow must consider these practices and build off them to create a security environment appropriate for information exchange. Streamlining the data exchanges between these large systems affords the opportunity to apply best practices more uniformly across the enterprise.

1.2.1.5 Data Standards

The overwhelming bulk of data exchanges occur as FTP-based flat file transfers in batch with file layouts being specific to the needs of each particular interface. Exceptions to this include protective order transactions restructured as message switch transactions, pre-sentence investigation interfaces using structured query language (SQL) against an intermediate staging database, parole and probation inquiries of ICON via Kaleidoscope, real-time driver's license, vehicle registration, and reciprocity inquiries utilizing eXtensible Markup Language (XML) as well as Livescan/AFIS transactions. What is lacking is a common data standard for these exchanges. The use of XML is not a foreign concept to any of these major State participants, and all have, in some form or another, approached the use of it in updating their existing interfaces. However, the efforts have been isolated from each other and usually utilize a markup scheme specific to the particular systems involved. To move forward with an integrated justice effort, a common, XML-based data standard will need to be the norm rather than the progressive exception, inclusive of the Global Justice XML Data Model (GJXDM) standard model.

These major participants can technically do this already to some extent. What remains is to coordinate an analysis of these exchanges so that a common data standard germane to all can be utilized.

1.2.1.6 Transaction Processing Capability

Transaction-based data exchanges are the exception rather than the rule in these major participants' current systems interfaces. However, the exceptions to that trend demonstrate significant promise with regard to cross-agency justice information sharing in Iowa. This is especially evident with the DPS exchanges with the DOT Driver's License, Vehicle Registration, and Reciprocity systems as well as the Livescan/AFIS processing. It is also in place to an extent with protective order entry.

A serious effort in analysis, design, and development will be necessary to not only identify the necessary event triggers to drive transaction-based processing but, in general, to elevate all of these systems' interfaces from the current batch-mode processing to real-time, event-driven transactions. In other words, while the CJIS Advisory Committee has identified through the Exchange Analysis studies the points in the justice process where events trigger exchanges, they must identify where in the individual information systems the triggers occur. Inroads have already been made from the examples given, and from a technical perspective, this is a logical enhancement and extension to a technical direction already being set forth.

1.2.1.7 Adoption of Web Service/SOA Standards

Service-oriented architecture (SOA) describes an application architecture in which all functions, or services, are defined using a description language and have interfaces that are "called" to perform business processes. Each interaction is independent of each and every other interaction and the interconnect protocols of the existing systems that participate in the SOA are based on open source languages such as XML.

SOA is not currently being used in these major State systems as most data exchanges are done as scheduled batches. Additionally, some existing transaction-based exchanges such as Protective Order entry, while they occur real-time, represent a more specific implementation of data transfer methodologies rather than the consistent use of a service-oriented architecture. Existing data exchanges between DPS and the DOT Vehicle Registration and Reciprocity systems are already web service-based and represent an established implementation. From a technical viewpoint, moving towards a service-oriented architecture is not so much a question of why or when for these major participants, but rather how it is best implemented. With the Open FOX message switch moving towards handling web-services this year, a significant piece of existing data exchanges (as they apply to DPS systems) can be moved into the service-oriented architecture model. The technical skills are already able to be leveraged by these participants; however, the design, analysis, and development effort necessary to enhance these existing systems and their existing interfaces will be serious.

1.2.1.8 Summary

In summary, the information systems employed by the State Court Administrator's office, the Department of Corrections, the Department of Public Safety, the Department of Transportation, and the Criminal Juvenile Justice Planning division are already exchanging data. They are already aware of the current limitations of these interfaces in that they grasp the design and nature of the transaction-based and workflow-driven architecture of an enterprise-wide integrated justice implementation. Updates to existing systems in terms of utilizing service-oriented architectures and transaction-based processing will be necessary and do not represent a trivial amount of work or coordination. Additionally, the inroads established in the use of XML need to be expanded to utilize a common XML-based data standard across the enterprise. Again, this will be a significant effort in analyzing existing interface formats and moving them to a general data standard such as the GJXDM model. However, for these major participants, these efforts are natural extensions and enhancements of the existing vision for the future of these systems.

1.2.2 To-Be Enterprise Description

The To-Be Enterprise Description section will provide the detail of what business initiatives, agreements, practices and processes will need to be established if the CJIS initiative is to be achieved in Iowa, as well as the technical environment we propose to take Iowa into the future. Much of the section will address how to fill the gaps that currently exist, which may be barriers to integration. These gaps were originally identified in the As-Is Business Assessment.

1.2.2.1 General Concepts for the Justice Enterprise in Iowa

The State of Iowa has made great strides over the past several years in planning for cross-agency criminal justice information sharing. An active governance structure has been established and the State has undertaken several studies that recommend strategies for integration.

However, to move to a fully integrated statewide approach to criminal justice information sharing, several enterprise-wide issues will need to be addressed. As has been well documented, among the State's 99 counties there are significant variations in business practices and forms used in the exchange of information. This results in disparities in the manner in which information is collected and shared, thus making the ability to electronically share the information far more difficult. In addition, there is currently no framework available to all agencies by which information can be exchanged in any coordinated way; each automated exchange that has been implemented has been negotiated specifically between the affected agencies.

To overcome these challenges, the MAXIMUS/URL Team proposes a strategy that includes the following components:

- The creation of an empowered governance, organizational, and project management structure that promotes the oversight and management necessary to move from CJIS planning to implementation;

- Adopt SOA to allow for an integration framework based upon industry open standards (WS-I), which will still maintain system autonomy through the exposure of loosely coupled services;
- A centralized CJIS integration or messaging Broker[6] and business process manager to facilitate the exchange of information between agencies that is mindful of disparate security policies and uses the commonly accepted GJXDM-conformant schemas;
- The incorporation of key identifiers into workflow documents to provide for the ability to track a person, incident, or case throughout the justice process;
- The promotion of standardized business practices and forms among practitioners;
- Leverage automation efforts within the justice community, such as the common charge table that the County Attorneys are preparing for their common case management initiative;
- Adoption of GJXDM as the State's data standard for information exchange
- The development of a standard Iowa justice domain model, through the creation of a statewide common GJXDM subset and extension data model and dictionary for information that is shared between the participating systems and necessary for automated processing to occur;
- Use of the ICN as the Iowa CJIS Solution network backbone where allowable by state statute;
- Build off of the successes that Iowa has previously demonstrated in automating exchanges, such as the protection order exchange, and the PSI exchange; and
- The use and expansion of the Department of Transportation's TraCS in an SOA environment as a manner in which electronic filing with the Courts can occur, both for law enforcement and County Attorneys.

The vision of the strategic criminal justice enterprise must include proactive steps for transition from a world in which automation is largely nonexistent or happens on a nightly basis through batch FTP exchanges to one where information is exchanged on a real-time basis, as a part of day-to-day workflow activities. From a business process perspective, this will require a shift in thinking about workflow and consensus on how to

[6] This CJIS Broker, described in detail in the To-Be Technical section of this document, manages the messaging non-functional requirements (i.e., gets information where it needs to be when it needs to be), is secure and from an authenticated source and manages business flow based on rules and content of messages. Agencies simply need to know what they want to accomplish from a business perspective and what rules the Broker will enforce to move the message (exchange) along. This will result in the sharing of the right information at the right time and will improve the quality and integrity of information within the enterprise.

direct the technical modifications to both maintain and improve the business operations of the agency as a result of the automation.

1.2.2.2 To-Be Business Recommendations

The recommendations for the Iowa integrated justice environment fall under several categories: Governance/Project Management, General Workflow, Addressing Disparity in Automation, Standards, Common Business Forms and Practices, Traceability, and Expanding the Number of Automated Exchanges. Each of these categories and the specific recommendations are addressed below.

1.2.2.2.1 Governance/Project Management

Because the implementation of CJIS will require a solid infrastructure for management, governance, and funding, there are several recommendations that the MAXIMUS/URL Team has made in this area. For example, in the area of governance, the Team has made the following recommendations:

- Expand the CJIS Advisory Committee to include a DOT representative;
- Recognize the role of the Planning Committee (subset of the CJIS Advisory Committee with stakeholders from large State systems) as the organization that provides direction for the CJIS implementation effort and project management team;
- Provide ongoing direction for the management and necessary resources for CJIS implementation in Iowa;
- Create and recognize the CJIS Program Office and allocate appropriate authority consistent with those recommendations; and
- Address issues around legal ownership of data and information included in the CJIS solution.

1.2.2.2.1.1 Organization and Project Management

The MAXIMUS/URL Team recommends that the CJJP coordinate the CJIS activities and the CJIS Broker, at the direction of the CJIS Advisory Committee, with support from the Information Technology Enterprise (ITE). Specifically, we recommend that CJJP and ITE enter into interagency agreements to manage the relationship and that a CJIS Program Office is created within CJJP. We envision CJJP acting as the body that directs and manages all program, business-related, and technical policies and activities under the direction of the CJIS Advisory Committee and CJIS Board. We envision ITE supporting the CJIS effort technically, as directed by the CJIS Program Office, by hosting the CJIS Broker and providing programming support and other maintenance-related activities.

Because ITE provides broad technical support to Executive Branch agencies and procures its own rules, standards, and procedures regarding information technology in Iowa, the interagency agreement that supports the relationship between CJJP and ITE would need to include provisions that ensure the direction set forth by the CJIS Advisory Committee

can be fully implemented by ITE. In some instances, the CJIS effort may need to request an exemption from the newly created Chief Information Officer (CIO) Council from specific standards if deemed in the best interest of the CJIS effort by the Board and Advisory Committee.

With regard to project management, the MAXIMUS/URL Team also proposes that the CJIS Project Manager is given authority to proactively conduct project management activities, including hiring staff and/or contractors to complete the work.

1.2.2.2.1.2 Funding

With regard to funding, the Team made the following recommendations:

- Allow the CJIS Program Office to continue soliciting grant funds to support CJIS implementation activities, including requesting a general fund appropriation from the Iowa Legislature;
- Create budgeting authority in the CJIS Program Office to generate a yearly CJIS budget for presentation to the legislature;
- Allow for the conditioning of new grant funds for projects and initiatives that are consistent with the statewide CJIS Plan;
- Encourage the development of new justice technology activities be coordinated with the CJIS Plan.

1.2.2.2.1.3 Outreach

Finally, the MAXIMUS/URL Team recommends, consistent with the MOU Addendum , the creation of a multi-faceted communications strategy that leverages the CJIS Advisory Committee, professional associations, and other methods to disseminate information from practitioners regarding the statewide CJIS effort in Iowa.

1.2.2.2.2 General Workflow

There were several recommendations made by the MAXIMUS/URL Team that would expand the current use of data exchange to transition to an environment in which data exchange was a part of day-to-day workflow and business process. To that end, the Team encouraged a transition to open standards, such as the adoption of service-oriented architecture (SOA) to support real-time data entry. The Team also recommends the use of XML technologies and specifically the GJXDM as the vehicle to describe information exchange between disparate systems.

The MAXIMUS/URL Team also recommends that the CJIS Program Office convene working groups to assist in the resolution of form and business process disparities among local agencies in Iowa. This standardization, coupled with the use of open source technologies and the adoption of data standards will maximize the number of organizations that can participate in the CJIS solution while keeping the costs as low as

possible. To build support for standardization and the associated business process changes, the Team recommends that Iowa's professional associations to assist in sponsoring standardization working group efforts, and communicating efforts to constituents.

Finally, the recommendations encourage a move toward electronic filing (e-filing) through the adoption of a digital signature to facilitate the process. However in Iowa, the State Constitution requires that any criminal filing include both the signature of the officer as well as a notary signature. In addition, non-scheduled criminal offenses require the notary to present a stamp or seal verifying the notarized signature. The notary signature issue is only applicable in criminal cases; the Iowa Judicial Branch is planning to implement e-filing in the Civil Court process in 2006, beginning with pilot projects. The Judicial Branch intends to use commonly accepted court filing standards (OASIS, XML) with this effort.

So while TraCS citation information populates ICIS, however, the Court still currently requires the paper citation as the official filing document, since the condition of the filing is the notarized signature.

To facilitate resolution of these issues and support the electronic exchange of filing information, the MAXIMUS/URL Team made the following recommendations:

- Provide Court rule or statute change to allow digital representation of authenticated signatures in ICIS to accept e-filing;
- Modify ICIS to accept digital signature, employing Public Key Infrastructure (PKI) security technologies to support the authentication of verified signatures necessary for criminal e-filing;
- Conduct business process review and change involved in accepting digital signatures and the need for independent verification of criminal complaints;
- Encourage all electronic court filing processes to use open architecture standards; and
- Request legislative modification to allow for an electronic certification to replace the stamp/seal requirement for the notary required for nonscheduled offenses.

1.2.2.2.3 Addressing Disparity in Automation

In order for all justice agencies to participate in the statewide CJIS effort, there will need to be a concerted effort to ensure access to automated information systems in all agencies. From our As-Is analysis, we have learned that there is an issue surrounding lack of automation for some County Attorney and Law Enforcement agencies in Iowa. It is also clear to us that there are efforts underway, such as the County Attorney Case Management Project that mitigate the effects of this situation. In addition, the Department of Transportation's TraCS system is in use in a number of local law

enforcement agencies and could be leveraged as a manner for these smaller agencies, without RMSs to participate in the statewide integration effort.

What must be better understood is the status of technology in these agencies, especially among local law enforcement agencies. In addition, the existing capacity of larger agencies that have their own CMS or RMS and their ability and willingness to modify those systems with interfaces that become the common standard for charging and electronic filing must be determined over the course of the CJIS implementation in Iowa.

To that end, the Team has made the following recommendations for local law enforcement and County Attorneys:

- Leverage TraCS to augment local law enforcement automation, to allow it to support all law enforcement agency e-filings, Citations and Complaints, and Incident Reports for agencies that do not have their own RMS.
- Create an XML Information Exchange Package Document (IEPD) for important law enforcement and prosecutor documents. The IEPDs describe a set of data that is transmitted for a specific business purpose. The XML will be common and can support agency preference (TraCS or RMS) for information sharing, since the XML is flexible enough to be used by all agencies, notwithstanding what system they use to participate in the CJIS solution .
- Continue CJJP support of the County Attorney CMS initiative to continue developing the project with the statewide CJIS in mind.
- To support automated County Attorney filing, Prosecutors should have query access to charges initiated by any local law enforcement agency in TraCS if using their own CMS.
- Prosecutors without a CMS should have the capability to view information in TraCS and make charging decisions based upon the charges therein.

1.2.2.2.4 Common Business Forms and Practices

As discussed in brief above, a move toward a common data standard and consistently used IEPDs requires that forms and practices in Iowa become more standardized. To that end, the MAXIMUS/URL Team has made the following recommendations:

- Leverage the planned TraCS OWI Complaint form for reusability across other non-traffic offenses;
- NIBRS-compliant Incident Report TraCS has developed should be considered for statewide use across offense types;
- Create important forms and documents – for both TraCS and other RMS – using standardized GJXDM schemas, enumerations and style sheets; and
- Create a rule-based exchange for charging documents.

1.2.2.2.5 Traceability

The ability to trace relationships between incidents, cases, and people is integral to an automated workflow process in the criminal justice enterprise. Law enforcement may view a "case" based upon an incident or series of incidents being investigated. Charges may be brought against a suspect in that case, which may or may not result in an arrest. The County Attorney may choose to file a case based upon the charges originally brought by law enforcement or may change the charges and file new or different charges with the Court. The Court opens a case based upon a filing and disposes the case. All of this can occur without a positive identification number or DCI#, and all of this can occur without a Document Tracking Number (DTN), but none of this will occur without each agency having its own case number and identifying the person by some name.

However, without a DCI#, DTN, or other universally accepted and understood tracking numbers the ability for justice practitioners to understand how an individual has interacted with the justice system over time and how each agency has been involved is limited. In addition, without tracking numbers tied to the information and supporting business rules, automated movement of information in the workflow will still require human intervention and in some cases actually increase the workload.

In Iowa, there are several ways that traceability could be improved, such as:

- Providing the DCI# back to the law enforcement agency as soon as the individual is booked on AFIS;
- Expanding DTN concept to all charge initiation events;
- Incorporating these identifiers into law enforcement charging documents, notwithstanding whether prints have been taken; and
- Including affidavit information on standardized complaint form to facilitate e-filing.

1.2.2.2.6 Expanding the Number of Automated Exchanges

Finally, the MAXIMUS/URL Team recommends that the Iowa CJIS effort begin to expand the number of exchanges that are currently automated, to include implementing an automated warrants exchange, as well as providing court disposition information in real-time to other justice agencies. A timeline for these and other exchanges are discussed in detail in the implementation plan sections of this document.

1.2.2.3 To-Be Technical Recommendations

The recommendations for the technical environment include, at the highest level, the adoption of a service-oriented architecture, implementation of a centralized CJIS Broker to facilitate information sharing, the use of the ICN as the Iowa CJIS solution network backbone, and the adoption of GJXDM as the State's data standard for information exchange.

1.2.2.3.1 Adoption of SOA

Service-oriented architecture describes an architecture in which one entity (computer) performs a defined measurement of work on behalf of another entity across a distributed computing environment regardless of the system platform. The MAXIMUS/URL Team recommends the adoption of the SOA model for facilitating complete, accurate, and timely information sharing in the Iowa CJIS environment. The SOA model provides the Iowa CJIS initiative greater flexibility than any of the other options. It establishes an open architecture environment for information sharing independent of the computing platforms deployed in that environment and has widespread support in the criminal justice community. The SOA model is the recommended approach of the Global Infrastructure/Standards Working Group[7] and was unanimously selected by Global Justice Information Sharing Initiative (Global) Advisory Committee as a framework for achieving justice integration.

1.2.2.3.2 Centralized CJIS Broker

A centralized CJIS Broker assists in the facilitation of justice information exchange among disparate systems by both managing the messaging of non-functional requirements (i.e., getting information where it needs to be when it needs to be) and ensuring that it is secure and from an authenticated source as well as managing business flow based on rules and content of messages. Agencies simply need to know what they want to accomplish from a business perspective and what rules the Broker will enforce to move the message (exchange) along. This will result in the sharing of the right information at the right time and will improve the quality and integrity of information within the enterprise.

There are several benefits to using the CJIS Broker as the centerpiece for the CJIS solution in Iowa. The solution supports independent agency development cycles and provides for a layer of abstraction between business systems and information exchange. The Broker provides each participating agency a single point to interface for exchanging information with all of their information sharing partners. This approach will relieve agencies of the burden to develop and maintain multiple interfaces, which can multiply exponentially if only one additional partner is added.

All of the State level and local level applications will require some amount of modification if they are going to implement new information sharing in an SOA environment with the CJIS Broker. Few applications in the current environment are configured for real-time, event-driven transaction generation and processing. Each will need to pursue a strategy to adopt a Transaction Architecture to be incorporated into their

[7] A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA), The Global Infrastructure/Standards Working Group, September 28, 2004.

current environment. Several options are available. At a minimum the strategy should take the following approach:

- Easily incorporated into the current system platforms;
- Leveraging transaction processing capabilities inherent in the system;
- Eliminating redundant capabilities to be supplied by the CJIS Broker; and
- Re-using and extending strategies that are successfully sharing information in the current application environment.

There are several functional requirements the CJIS Broker would be expected to perform to support the exchange of information from one agency to another, such as the translation of code values, maintaining a standardized charging table, assigning enterprise case and charge tracking numbers, allowing for registration for subscription and notification, as well as logging and auditing functions. In addition, there are important non-functional requirements to the solution that address user interface, security, scalability, and the business-processing environment. Each one of those issues will be addressed below.

1.2.2.3.2.1 User Interface

The MAXIMUS/URL Team recommends that the web portal and user interface, or the screens with which the user interacts, is custom developed for the CJIS Broker using the screens of their native systems. This will help ensure that adequate security measures and policies are applied and also reduce the dependencies on outside agencies for access to the Broker. This recommendation will leverage common operating platforms and infrastructure and avoid deployment of unnecessary features typically included in an off-the-shelf solution.

1.2.2.3.2.2 Security

There are several security requirements for the CJIS solution in Iowa, most of which are predicated on the assumption that current systems already implement a level of user authentication and access. The recommendations include:

- Large State systems will install firewalls to connect to the CJIS Broker;
- Remote users to the CJIS Broker will require a Virtual Private Network connection over the Internet;
- Procurement after September 30, 2005 shall require a minimum of 128-bit encryption with NIST, CSL Certification of the Cryptographic to meet FIPS Publication 140-2; and
- Procurements must comport with State of Iowa Enterprise Security Guidelines.

1.2.2.3.2.3 Usage and Scalability

Regarding capacity, usage, and the system's ability to scale to support more users, the MAXIMUS/URL Team recommends a CJIS Broker solution that has the capacity to scale processing load, and additional participants, with a low impact on existing users. As further discussed in the implementation strategy and timeline section, we recommend a solution that provides for over maximum expected capacity at five years and can grow without reworking the existing configuration, since the plan is to bring more and more users and information exchanges onto the CJIS Broker over the course of the five years. The net result is a maintainable architecture capable of anticipated growth.

1.2.2.3.2.4 Business Processing Environment

The MAXIMUS/URL Team recommends using a J2EE Platform, which is flexible in an environment with multiple hardware platforms and operating systems.

1.2.2.3.3 ICN Backbone as the To-Be Network Solution

The MAXIMUS/URL Team recommends using the Iowa Communications Network (ICN) as the telecommunications infrastructure for the Iowa CJIS environment. In the short-term, the Team recommends the use of the existing ICN wide area network (WAN), even though it limits service to state agencies and excludes local and county entities, namely the County Attorneys. In the long term, we recommend mandating the use of the existing ICN WAN to support justice data exchanges within the State of Iowa. The advantages of leveraging the ICN infrastructure is that it is already in use by most of the CJIS participants in the state. In addition, there is connectivity in every county, notwithstanding the "last mile" requirements for connecting with agencies using local telecommunications providers.

1.2.2.3.4 GJXDM Data Standards

The GJXDM is a flexible yet comprehensive set of data standards to drive the specifications of the data exchanges for the Iowa CJIS solution. The key to developing a long-term, open, and workable data standard is using is using the GJXDM and requiring its use among all agencies that participate in the automated solution. This is precisely the benefit of using the GJXDM; all agencies that intend to integrate can use the single GJXDM-conformant schema that is developed for a particular exchange instead of developing their own in a vacuum. Iowa-specific IEPDs that are GJXDM-conformant will be the structure for all data exchange formats.

1.2.3 Integration Plan Overview

The Integration Plan Overview will identify the high-level strategy, timeline, costs, and risks necessary to move from the "As-Is" environment to the envisioned "To-Be" environment.

1.2.3.1 Integration Strategy

The approach that the MAXIMUS/URL Team has taken in putting together the strategic implementation plan focuses on leveraging existing systems and incremental implementation, using proof of concepts and pilots to demonstrate results quickly and create infrastructure for future development.

The following are specific assumptions about our approach to the implementation strategy and this document:

- The strategic plan is based on current systems: the CJIS plan is intended to facilitate the exchange of information between existing systems and in no way replace their functionality.
- The order of activities in Years One through Five are important and based upon our best thinking about the necessary infrastructure that must be created early on, and as such, there are dependencies between and among tasks. In other words, tasks cannot be pulled out randomly or disregarded without there being a possible ripple effect upon the expected outcomes of the plan as it is written.
- In the cost section of the document, we have defined a low-end and high-end estimate. The labels of "low" and "high" are not intended to denote a superior solution; rather they are referring to the cost of the category. Typically additional cost adds additional performance for the category denoted, but the requirement for that performance in the Iowa CJIS solution should be driven by the detailed requirements.
- Budget estimates include operational and labor costs, in addition to hardware, software, and maintenance costs.
- While the MAXMIUS/URL Team has compiled a great deal of information about grants and funding to support CJIS efforts, it is essential for an implementation of this scale to be supported at the State and local levels. We strongly encourage the CJIS Board and Advisory Committee to work with the Iowa Legislature in preparing a budget request for general fund appropriations to support ongoing CJIS implementation.

1.2.3.2 Integration Timeline

This section outlines the recommended implementation timeline for the Iowa CJIS solution over the next five years. The recommendations are presented by Fiscal Year (FY), and Year One is considered to be FY 06, beginning July 1, 2005. The MAXIMUS/URL Team understands that is too soon to have received a new general fund appropriation for CJIS, however it is crucial that momentum not be lost waiting a year for new funding. Significant work can be undertaken in the first year, while aggressive, and nevertheless can be done before the significant project costs are incurred.

CJIS planning has already completed an extensive amount of work over the past few years as outlined in the previous sections. As noted, there have been significant strides

made, and it is this momentum that needs to be maintained. Although the timeline reflects the current year as Year One, in actuality it may be seen more broadly as entering the first year of the development and implementation phase of CJIS.

The costs that are associated with the implementation timeline will vary as timelines shift in future years. The costs also reflect a high/low estimate, as it is difficult to precisely determine specific costs without the State having made decisions based upon recommendations laid out in this plan. The low-end costs often reflect what the MAXIMUS/URL Team believes the State would require to meet the incremental goals of the project; the high-end would meet these goals while mitigating the State's risk by providing room for unforeseen issues in implementation and a more technically robust environment.

The hardware and software that will make the electronic exchange of information possible both at the agency level and at the CJIS level is intended to facilitate the exchange of information between existing systems and in no way replace their functionality or build a new justice "system". But as CJIS becomes operational, the agencies will depend more and more upon its availability and reliability and will come to expect it to perform at least as equally well as their own. We have accounted for this increase in expectation for availability in the high-end numbers, and while we suggest this is realistic, there is an incremental approach the State may take in bringing on the fully operational environment.

The recommended tasks and timeline are just that–recommendations; they do not presume to imply an "all or nothing" approach. However, it is important to understand that many tasks are dependant upon other tasks having been completed or begun. In other words, tasks cannot be pulled out individually without there being an effect upon the expected outcomes of the plan as it is written. Some tasks and their ordering are critical; others may be delayed, reordered, or not undertaken at all without having a major impact upon the CJIS project as a whole. There are of course alternatives to the prescribed solutions for a specific goal which may also be substituted without consequence, while other changes may pose a significant enough change to make the plan as written weaker. How the various tasks fall regarding these categories may be readily apparent and for others will require further analysis.

The following table describes the specific activities that the MAXIMUS/URL Team recommends for each of the five years.

Year (FY)	Recommended Activity/Task
Year One (06-07)	Governance and Project Management activities: • Establish CJIS Program Office • Create MOUs between CJJP and ITE • Add DOT to the CJIS Advisory Committee • Exemption from Technology Governance Board
	Conduct business process review of e-filing issues for criminal cases.

	Create a legislative package that includes the business case for integration and a funding request for FY 07-08. Introduce performance measures for justice information sharing and tie performance to future funding requests.
	Conduct transition to SOA environment with the following pilot exchanges: • Uniform Traffic Citation and Complaint • PSI • Protection Order
	Develop GJXDM-conformant information exchange packages (IEPDs) to facilitate exchange of Year One documents. Begin building Iowa-specific GJXDM-conformant namespace and data standards (ongoing).
	Conduct transaction processing analysis, or the process of identifying "trigger events" that will initiate discrete web services to support Year One exchanges.
	Begin web services implementation by establishing the ability to create or consume a SOAP message. Focus on State agencies participating in Year One exchanges.
	Establish and procure security protocols: VPN for remote users and firewalls in and out of large agency systems to connect to CJIS Broker (Year Two).
	Begin developing IEPDs for Year Two documents: Complaint and Affidavit, Trial Information, and Incident Report, Warrant, and if time permits, begin work on OWI Exchanges and Sentence Orders.
	Create RFP for CJIS Broker (assumes a FY 07-08 appropriation).
Year Two (07-08)	With the funds appropriated from the legislature, hire three additional staff members for the CJIS Program Office (Justice Business Domain Modeler, CJIS Help Desk, and CJIS Software Developer).
	Release the RFP for the CJIS Broker, complete procurement and implementation during Year Two
	Convert Year One pilot exchanges to SOA environment.
	Shift to web services at local level by expanding County Attorney Case Management Project and identifying local Law Enforcement systems that are able to participate in the CJIS Broker solution.
	Ensure that TraCS has the ability to send and receive SOAP messages and has persistent data storage.
	Create the user interface application in TraCS for County Attorneys to access charging documents.
	Continue building Iowa-specific GJXDM-conformant namespace and data standards (ongoing).
	Conduct transaction processing analysis, or the process of identifying "trigger events" that will initiate discrete web services to support Year Two exchanges.
Year Three (08-09)	Expand licenses to new State agencies (Attorney General, Public Defender).
	Continue CMS/JMS/RMS ability to participate in web services at the local level.
	Identify "lessons learned" from the process behind establishing new exchanges in Years One and Two.
	Pilot Year Two Exchanges (Complaint and Affidavit, Trial Information, and Incident Report, Warrant, OWI Exchanges, and Sentence Orders).
	Conduct Business process and transaction processing analysis: • No Contact Order Process • Publish/subscribe type notifications • Hearing Court Orders, Notice of Court Date • Expungement • Detention (e.g., Release, Bond Order)
	Continue building Iowa-specific GJXDM-conformant namespace and data standards (ongoing).

Year Four (09-10)	Continue CMS/JMS/RMS ability to participate in web services at the local level.
	Pilot Year Three Exchanges (No Contact Order, Hearing Court Orders, Notice of Court Date, Expungement, and Detention documents).
	Conduct Business process and transaction processing analysis: • Appellate Process • Juvenile Formal Adjudication Process • Motions • Supervision • Pre-Trial Supervision
	Continue building Iowa-specific GJXDM-conformant namespace and data standards (ongoing)
Year Five (10-11)	Continue CMS/JMS/RMS ability to participate in web services at the local level.
	Pilot Year Four Exchanges (Appellate Process, Juvenile Formal Adjudication, Motions, Supervision, Pre-Trial Supervision).
	Conduct Business process and transaction processing analysis: • Diversion • Juvenile Informal Adjustments
	Continue building Iowa-specific GJXDM-conformant namespace and data standards (ongoing).

1.2.3.3 Integration Plan Cost

The Integration Plan Cost section outlines the one-time implementation costs, the recurring operational expenditures, and the spending rates for both categories over the five-year CJIS Integration Plan. The costs presented are intended to provide the CJIS Board, CJIS Advisory Committee, and Iowa CJIS Program Office pricing information to assist in planning and budgeting for achieving the CJIS initiative.

In addition, the document presents a range of costs, as a low-end and a high-end estimate. The pricing presented is a cost range based upon known industry items in the category of cost being portrayed in each section and provides a low-end solution versus high-end solution implementation. The labels of "low" and "high" are not intended to denote a superior solution; rather, they are referring to the cost of the category. Typically, the high-end cost adds additional performance for the category denoted, and in this model our high-end pricing reflects what would produce maximum performance. However, we encourage that the specific requirements for performance in the Iowa CJIS Solution be driven by the detailed requirements. The goal of the five-year integration plan is to implement the best solution for Iowa, which may not be the most expensive solution. The prices are based upon current item costs; however, there is no recommendation being made for the selection of a particular brand item.

The exact implementation costs will only be known as more detailed information about the cost category is determined in the later phases of the plan. The To-Be CJIS Solution presented earlier can be achieved with many combinations of tool, hardware, software, and labor components. The solution dimensions such as processing speed, expected availability, scalability, buying versus building the solution, will need to be assessed in a requirements analysis phase to determine the exact configuration and costs that will be necessary to implement the solution. The low-end and high-end architectures are

presented as separate diagrams. The intent is to show what each architecture would look like once fully implemented by the end of the five-year period. It is possible to envision an architecture where some components are not initially implemented up front (e.g., XML accelerators or full failover capacity implemented as clustered server solutions).

The implementation costs are those one-time occurring expenditures that will be necessary for the implementation of the CJIS Broker. Implementation includes the categories of hardware procurement, software procurement, and solution implementation. Each category presents a low-end versus high-end scenario, but does not infer that one solution is superior to the other. The particular expenditure for the categories will be based upon several factors to be determined during the five-year CJIS Integration Plan execution. These factors will determine what the best solution is for Iowa. Factors that need to be considered in the final cost scenario are:

- Detailed system functional requirements
- Detailed system non-functional requirements
- Iowa CJIS policies
- Iowa CJIS technology standards
- Available funding

These factors should be considered more fully in the initial stages of the five-year plan to ensure detailed costing scenarios can be created to drive the funding efforts of the CJIS Program Office.

Also, it is important to note that there is not a pure buy/cost scenario for the CJIS Broker being presented. While there are several consumer off-the-shelf (COTS) solutions that provide portions of the functionality necessary for achieving the State of Iowa CJIS initiative, there is not a single solution for all the functionality known at this time. Even if the State determines that buying particular components of the system as COTS items, integration of those components into a single solution will require some software development life-cycle activity.

The following summary chart depicts the implementation and operational costs for both the low and high-end solutions for the five years:

	Low-End Solution				High-End Solution			
Year	**Total**	**% of Project**	**One-Time Expenditure**	**Recurring Cost**	**Total**	**% of Project**	**One-Time Expenditure**	**Recurring Cost**
Fiscal Year 06	$357,666.42	6%	$261,377.70	$96,288.72	$690,804.88	6%	$569,466.85	$121,338.03
Fiscal Year 07	$1,963,416.90	33%	$1,607,356.93	$353,345.97	$3,888,015.83	32%	$3,387,417.21	$496,955.62
Fiscal Year 08	$1,892,040.70	32%	$1,471,268.98	$420,771.72	$3,657,149.05	31%	$2,881,466.76	$775,682.29
Fiscal Year 09	$889,786.35	15%	$447,499.48	$442,286.87	$1,961,875.78	16%	$1,089,852.90	$872,022.89
Fiscal Year 10	$882,511.15	15%	$421,872.43	$460,638.72	$1,791,673.42	15%	$842,554.38	$949,119.04
Total	**$5,985,421.51**	100%	**$4,209,375.51**	**$1,773,331.99**	**$11,989,518.97**	**100%**	**$8,770,758.10**	**$3,215,117.87**

1.3 Document Section Descriptions

The following 200 plus pages of this document describe in detail the process and methodology that the MAXIMUS/URL Team used to understand the justice environment in Iowa, and led to our conclusions and recommendations for the future CJIS environment in Iowa and how to implement our approach over the next five years.

Specifically, the document sections are as follows:

- *Section 2 – Introduction to Integrated Justice* describes what CJIS is, its evolution, and national standards and best practices around justice information sharing.
- *Section 3 – As-Is Business and Technical Readiness Assessment* describes our "As-Is" Business and Technical assessments, as well as the methodology we used to gather the information.
- *Section 4 – To-Be Iowa CJIS Description* discusses the "To-Be" environment and our recommendations for CJIS in Iowa.
- *Section 5 – Strategic Integration Plan* maps the "To-Be" to a five-year implementation schedule and also provides cost information for the effort.
- *Section 6 – Performance Metrics* discusses performance measures and how the State of Iowa can begin measuring the benefits of justice information sharing
- The appendices include local implementation costs, the list of questions used for the "As-Is" online survey, and a glossary of terms used in this document.

1.4 Conclusions

The MAXIMUS/URL Team are confident that the CJIS integration plan will provide the CJIS Board and Advisory Committee with the direction it needs to move forward with criminal justice information sharing in Iowa.

2 Introduction to Integrated Justice

The Introduction to Integrated Justice section will provide a foundational description of criminal justice information system (CJIS) in general terms, identifying key concepts and the evolution of justice information sharing in the United States. This section will also identify and present best practices information from organizations such as SEARCH, NASCIO, and the U.S. Department of Justice, Office of Justice Programs (OJP), as well as information about established and emerging national standards that greatly assist implementing cross-agency information sharing.

2.1 Definition of CJIS

The key to understanding CJIS is to address it as an enterprise-wide issue, rather than something that one agency must undertake on its own. NASCIO, the National Association of State Chief Information Officers, defines this comprehensive approach as enterprise architecture that "provides an *enterprise view* – a comprehensive, holistic view of the enterprise that includes environmental understanding, explicit strategic intent, and the organization, business processes, *and* technologies that enable that intent. Enablers are capabilities that must be evaluated and prioritized. Capabilities are delivered or further leveraged through management initiatives, programs and projects."[8]

SEARCH, the National Consortium of Justice Research and Statistics, defines CJIS as "the ability to share critical information at key decision points throughout the justice enterprise."[9] Thus, the justice enterprise view describes how the justice system must define its environment – its enterprise – if it intends to share information in an automated fashion. According to the NASCIO report, "the justice enterprise alone includes numerous justice and non-justice agencies that operate a myriad of systems for collecting, maintaining, analyzing and sharing data and information critical to carrying out their respective missions. Creating the capacity to share information and data among and between agencies, levels of government and a variety of disciplines— indeed, creating an enterprise approach— means overcoming established barriers to data exchange. It involves understanding cross-jurisdictional information needs and the data and information exchanges that cross sometimes radically different lines of business."[10]

[8] *Government Information Sharing: Calls to Action, Volume 1: Justice*, NASCIO, March 2005, page 7 (hereinafter *NASCIO Calls to Action*).
[9] *A Common Understanding*, page 9.
[10] *NASCIO Calls to Action*, page 11.

2.2 Concepts of CJIS

According to a National Criminal Justice Association study on governance structures completed in 2001, there are several ways to describe what CJIS means to the everyday justice practitioner:

> *Justice information systems integration describes a broad range of interagency, interdisciplinary, and intergovernmental justice information sharing improvement initiatives that may vary widely in content from state to state.*
>
> *Integration, according to a state court administrator, envisions a world in which [justice] data is routinely shared across the criminal justice system and with the public." The integration mission, as one state official explained it, is to "allow an authorized user to access data, regardless of where that data is located."*
>
> *One state CIO described an integrated justice information system as a "mosaic [of information systems] that will fit together very well." That mosaic will be comprised of "pieces that can be lifted out [for operational improvements and enhancements] and plugged back in," but that collectively will remain an integrated system.*[11]

Bringing together information from disparate agencies requires adherence to commonly agreed-upon goals and objectives for the integrated justice environment. According to SEARCH, *Integration in the Context of Justice Information Systems: A Common Understanding*, there are several fundamental principles that underlie an integrated justice environment:

- Information is captured at the originating point, rather than reconstructed later.
- Information is captured once and reused, rather than re-captured when needed again.
- Integrated systems fulfilling these functions are comprised of, or derived from, the operational systems of the participating agencies; they are not separate from the systems supporting the agencies.
- Justice organizations retain the right to design, operate, and maintain systems to meet their own operational requirements. However, as with any network capability, participants must meet agreed-upon data, communication and security requirements, and standards in order to participate.

[11] *States' Governance Of Justice Information Systems Integration: Managing Decisionmaking In An Integrated Environment, Observations And Insights From The Field*, National Criminal Justice Association, 2001, page 6.

- Whenever appropriate, standards will be defined, with user input, in terms of performance requirements and functional capabilities, rather than hardware and software brand names.
- Security and privacy are priorities in the development of integrated justice capabilities and in the determination of standards.
- Integration builds on current infrastructure and incorporates capabilities and functionality of existing information systems, where possible.
- Because of the singular consequences of decision making throughout the justice enterprise, establishing and confirming the positive identity of the record subject is crucial.[12]

2.3 Benefits of Integration

The State of Iowa, in its RFP for the CJIS Integration Plan, made it very clear the benefits they expect to achieve from implementing integrated justice in the State:

- Better Decision-Making
- Reduced Redundant Data Entry
- Reduced Delays in the Flow of Information Between Agencies
- Improved Information Available to Agencies
- Improved Staff Productivity
- Reduced Paper Costs
- Reduced Dependence on Individuals With other Stakeholder Organizations
- Reduced Time Locating Information or Data
- Improved Data Integrity
- Improved Statistics for Policy Decisions

There are several reasons why the State of Iowa should expect to achieve these goals by implementing a statewide CJIS initiative. According to SEARCH, there are several benefits to automated, cross-agency justice information sharing:

> *Integrated systems improve the quality of information, and thereby the quality of decisions, by eliminating error-prone redundant data entry. In addition, by sharing data between systems, integration typically improves the timely access to information, a critical factor at many justice decision points (for example, setting bail). Moreover, integration enables the sharing of crucial information without regard to time or space; multiple users can access the same records simultaneously from remote locations around the clock. Integration also substantially improves the consistency and reliability of information, and enables immediate access by key decision makers.*
>
> *Errors in justice information can be greatly reduced by eliminating redundant data entry, which not only results in lower labor costs, but also significantly improves the quality of*

[12] *Common Understanding*, page 9.

> *justice — an intangible that too often is measured by the size of civil suits resulting from improper confinement, improper release or other errors traceable to poor data quality or untimely access to critical information.*[13]

Benefits of this nature are identified, understood, and can be measured by undertaking a series of steps. First, it is critical to understand how and why these benefits are not being achieved in the current business and technical environment, and if they are, what has helped facilitate their realization. Second, it is imperative that the State consider the performance measures necessary and appropriate to measure these benefits both prior to and post-CJIS implementation.

This analysis attempts to address both steps. The benefits and how they align with the As-Is process in Iowa is discussed in Section 3. We also provide guidance to the State in establishing performance measures in Section 4.

2.4 Evolution of CJIS

The concept of passing justice information from one agency to another in an electronic format is not a new concept. The first implementation of this nature was borne from the need to share criminal history information between states through the National Crime Information Center (NCIC), which is managed by the U.S. Department of Justice, Federal Bureau of Investigation. The creation of NCIC, which was established in 1967, was a significant accomplishment in that it created the first message-based transaction handling system for which there was a single set of communications protocols and data exchanges that described how states would interoperate with NCIC.

The NCIC information exchange among law enforcement agencies at the local, state, and federal level has been replicated for several different law enforcement-related activities, such as the exchange of fingerprint information through Integrated Automated Fingerprint Identification System (IAFIS), driver's license information through the National Law Enforcement Telecommunications System (NLETS), and criminal history background checks to authorize firearms purchases through the National Instant Check System (NICS). These exchanges between levels of government are sometimes called vertical integration.

Horizontal information sharing is a more recent trend in CJIS. It refers to the ability of information sharing and access extends across agencies and branches of government at the state and local level.[14] To facilitate and promote horizontal information sharing among justice agencies and to advise on policy issues around justice information sharing, the Justice Department created a Federal Advisory Committee (FAC) called the Global Justice Information Sharing Initiative (Global), which has as its mission to improve the administration of justice and protect the public by promoting practices and

[13] *Common Understanding*, page 4.
[14] *Ibid.*, page 5.

technologies for the secure sharing of justice-related information. To achieve that end, Global undertakes the following activities:

- Bring together representatives from the entire justice community and related entities—including private industry—to overcome the barriers to justice information sharing across agencies, disciplines, and levels of government.
- Promote the development and implementation of standards that facilitate seamless exchange of information among justice and related systems.
- Provide information that supports sound business decisions for the planning, design, and procurement of cost-effective, interoperable information systems.
- Promote constitutional values and individual rights by ensuring the accuracy and security of justice information, and the implementation of appropriate privacy safeguards.
- Recommend concepts that leverage existing infrastructure, capabilities, and functionality.[15]

As a FAC, Global meets twice a year and is supported by the Justice Department's Bureau of Justice Assistance (BJA). In its short history, Global and BJA have undertaken a variety of important initiatives, including: the creation and support of the Global Justice XML Data Model (GJXDM); the creation and support of functional standards for corrections, law enforcement, court, and prosecutor agencies; addressing privacy and policy issues associated with justice information sharing; providing guidance through documents and training on planning, governance, and making the "business case" for information sharing; and creating opportunities for agencies implementing integrated justice to share information with others and learn from one another.

Information about Global, BJA, and these initiatives may be found at www.it.ojp.gov.

2.5 Common Barriers to CJIS

Generally speaking, there are several barriers to sharing information electronically across agencies. A significant barrier is policy, and the rules around storing and sharing information. Traditionally, electronic information has been protected and contained within a specific agency system. To share information electronically requires a change in agency policy in that regard and the development of trusted relationships among agencies that share information and agreement as to the specific information that is passed and the circumstances under which information is shared. In some cases, information sharing may also be restricted by state law, in which case legislative change may be necessary.

[15] *Global Justice Information Network Annual Report 2002*, page 3 at http://it.ojp.gov/global/outreach/37/global_report_2002.doc.

In addition to policy and legislative issues, funding has been a common barrier to CJIS implementation. While a commonly accepted principal of justice information sharing is that justice organizations maintain their own information systems and retain the right to design, operate, and maintain those systems to meet their own operational requirements, there is a cost associated with the technology and programming necessary to support the electronic exchange in information. This trend in integrated justice has occurred, unfortunately, at the same time that available discretionary state and local funding declined, due to budget shortfalls. As such, there are significant funding barriers to justice information sharing.

A related barrier is the level of technology currently in use – or lack thereof – within the agencies participating in the integrated justice solution. For example, many information systems in use by justice agencies are proprietary and not able to adapt to open source standards that facilitate information sharing. Furthermore, some agencies – especially smaller agencies and those in rural areas – may not be using information systems to manage records or cases, or may not use automation at all. Getting these organizations to the point where they can participate in an integrated justice solution will take a significant investment of both time and funding.

A final issue is more subjective and has to do with the organizational dynamic as a barrier to information sharing. Traditionally, information has been associated with power, and even in circumstances in which there is no policy or legislation that prevents the exchange of information, there is sometimes resistance to sharing information. This matter can be overcome through education and outreach, as well as the ability to measure and quantify the benefits associated with integrated justice.

2.6 National Requirements

According to information provided by BJA, the Global Justice XML Data Model (Global JXDM or GJXDM) is an object-oriented data model for organizing the content of a data dictionary (the Global JXDD) in a database. The GJXDM began in March 2001 as a reconciliation of data definitions evolved into a broad endeavor to develop an XML-based framework that will enable the justice and public safety communities to effectively share information at all levels of government—laying a foundation for local, state, tribal, and national justice interoperability.[16]

From this database, an XML schema specification can be generated that consistently represents the semantics and structure of common data elements and types required to exchange information within the justice and public safety communities. In August 2002, the Global Justice Information Sharing Initiative (Global) Infrastructure and Standards Working Group (GISWG) formed the XML Structure Task Force (XSTF) to identify data requirements, explore XML concepts, and apply XML best practices to design and implement GJXDM. The XSTF is a working group composed of government and

[16] *Global Justice Information Network Annual Report 2003*, page 12 at http://it.ojp.gov/documents/2003_Global_Annual_Report.pdf.

industry domain experts (from law enforcement, courts, corrections, etc.), technical managers, and engineers.

The purpose of the Global JXDM is to provide a consistent, extensible, maintainable XML schema reference specification for data elements and types that represent the data requirements of the general justice and public safety communities. A secondary goal is to provide a baseline model for the data dictionary that can be represented in advanced technologies independently of XML schema. In January 2004—after years of development, testing, and refinement—Global released the first operational version of the Global JXDM, Version 3.0, to the justice community.[17] At the time of this report, the GJXDM is at version 3.0.2, with 3.0.3 soon to be released. The Justice Department expects that release 3.1 will be out within the next six months.

Currently, BJA is conditioning federal grant funds for the implementation of CJIS efforts on the use of the GJXDM.

In addition to the GJXDM, there are several other national initiatives to promote integration through the creation of functional and technical standards for disciplines in the justice community. Examples of these efforts include:

Law Enforcement Information Technology Standards Council (LEITSC). LEITSC is a consortium of four of the nation's leading law enforcement organizations, specifically, the National Organization of Black Law Enforcement Executives (NOBLE), National Sheriffs' Association, Police Executive Research Forum (PERF), and International Association of Chiefs of Police. The mission of LEITSC is to foster the growth of strategic planning and implementation of integrated justice systems by promoting the merits of information technology standards and providing advice to the nation's law enforcement community on technical aspects of IT standards. One of the primary efforts of the group has been to develop functional standards for Records Management Systems (RMS) and Computer Aided Dispatch (CAD) Systems.

Court Standards. The National Center for State Courts (NCSC) has long been a leader in the development of both functional and technical standards for courts. Under the leadership of the Conference of State Court Administrators and the National Association of Court Managers, functional standards for criminal, civil, traffic, domestic violence, and juvenile courts have been developed, as well as standard processes for electronic filing. These functional standards are currently in the process of being updated.

In addition to the business standards, NCSC has also taken the lead in supporting technical standards for the courts. It has created a GJXDM navigation tool called Wayfarer, which provides a hierarchical overview of the model relationships and provides detailed information about individual elements and types and the relationships between them. NCSC is also supporting the creation of GJXDM-conformant reference

[17] GJXDM Frequently Asked Questions page at http://it.ojp.gov/jxdm/faq.html#N10036.

documents for important court documents and developing GJXDM Information Exchange Package Documentation (IEPD). These IEPDs consist of domain data models, mappings to the GJXDM, schemas, and documentation all meant to be a guide for the courts in developing their application-specific GJXDM-conformant schemas, with a goal of making a consistent mapping to the GJXDM readily available the courts community.

Corrections Standards. In 2003, the Corrections Technology Association published functional standards for corrections management systems. The standards include offender management, medical, program management, property, and community supervision business functions.

Prosecutor Standards. The Prosecutor Exchange Project Steering/Advisory Committee, convened by the IJIS Institute and the National Association of Justice Information Sharing (NAJIS), is currently working to develop technical XML standards for Prosecutor-related documents that map to the GJXDM. Currently, the group is working on developing GJXDM Information Exchange Packages components for the following documents issued by Prosecutors:

- Components for the information (bill of information), complaint, indictment, and petition (Juvenile)
- Warrants, Bond, and Summons
- Prosecutor Disposition
- Subpoenas

2.7 Iowa CJIS Overview

In Iowa, the CJIS initiative began in 2001, with the creation of a Memorandum of Understanding (MOU) between the Governor and the Chief Justice of the Supreme Court. It created a CJIS Board including the Governor, the Chief Justice of the Iowa Supreme Court, the Director of the Department of Administrative Services or his or her designee, and the State Court Administrator. The duties of the Board are to review recommendations submitted by the Advisory Committee and set policy for the State relating to all aspects of an integrated criminal justice information system, including design, development, funding, implementation, and operation. The Board may adopt or disapprove the recommendations of the Advisory Committee.

The Advisory Committee is the active working group overseeing the CJIS initiative in Iowa. According to the MOU, the Advisory Committee shall be composed of the following members:

- Four representatives of the Judicial Branch appointed by the Chief Justice.
- Four representatives of the Executive Branch appointed by the Governor.
- One representative of each of the following associations: Iowa County Attorney's Association, Iowa State Sheriff's and Deputies Association, Iowa Association of

Chiefs of Police and Peace Officers, Iowa League of Cities, and Iowa State Association of County Supervisors. The leadership of each association shall appoint the association's representative.

- Two members of the Iowa Senate, including one Democrat and one Republican, each to be appointed by the leadership of their respective caucus, to serve as ex-officio members.
- Two members of the Iowa House of Representatives, including one Democrat and one Republican, each to be appointed by the leadership of their respective caucus, to serve as ex-officio members.

At its inception, the Advisory Committee was charged with conducting an in-depth examination of the existing criminal justice information systems that exist or are being developed around the state and assess their capabilities from both a technological and a procedural perspective. From this examination, it was charged with making recommendations to the Board regarding policies in the areas of privacy, security, standards, planning, funding, operations, technology, architecture, legislation, and any other issues related to sharing criminal justice information among and between agencies.[18]

To that end, the Advisory Committee undertook a number of activities, including documenting the information exchanges that take place among criminal justice agencies in Iowa, as well as those that occur in the juvenile justice system. These studies documented the current workflow as well as process gaps and places where automation would greatly improve the administration of justice in Iowa.

In 2004, the MOU was amended to require the CJIS Advisory Committee to create a strategic plan to guide CJIS implementation in Iowa. Specifically, the addendum required the CJIS Integration Plan to be based upon interfaces and data transfers, and preserve existing information systems, procedures, and business practices of individual agencies. The MOU further states that the plan "may incorporate the use of a common case management system, procedures, and business practices of individual agencies with similar or common functions. However, CJIS shall not be a single, centralized system, nor is it intended to mandate the elimination or significant modification of individual agency information systems, procedures, and practices."[19]

[18] State of Iowa, Memorandum of Understanding: Criminal Justice Information System at http://www.state.ia.us/government/dhr/cjjp/images/pdf/finalCJIS_MOU.pdf (hereinafter MOU).
[19] Addendum to the Memorandum of Understanding: Criminal Justice Information System at http://www.state.ia.us/government/dhr/cjjp/images/pdf/CJIS%20MOU%20Addendum.pdf (hereinafter MOU Addendum).

3 As-Is Business and Technical Readiness Assessment

The As-is Business and Technical Readiness Assessment sections will provide a detailed examination and assessment of the readiness of the current and near-term business and technical environments of the participants expected to share information using the Iowa CJIS solution.

3.1 Methodology

This section will discuss the methodology we used for gathering information, both an online survey (including participation statistics, dissemination methodology, etc.) and the interviews with individuals who manage key State systems. The MAXIMUS/URL Team employed a variety of information gathering techniques to conduct the As-Is Technical and Business Readiness Assessment. First, the Team reviewed the following studies, which had been conducted previously:

- Adult Exchange Modeling Report
- Juvenile Exchange Modeling Report
- Pre-Trial Sentencing Investigation Report
- Draft State of Iowa Security Policy
- County Attorney and Jail Management Survey
- SEARCH Reports from 2000 and 2002

3.1.1 Interviews

The second information gathering technique was to conduct interviews with key State system stakeholders. During the week of May 9, 2005, the MAXIMUS/URL Team met with the following State officials:

- Tuesday, May 10th
  Larry Grund, DPS (IOWA System, Kaleidoscope)
- Tuesday, May 10th
  Dick Moore, CJJP (Justice Data Warehouse)
- Wednesday, May 11th
  Mary Jensen, DOT (TraCS)
- Thursday, May 12th
  John Baldwin, DOC (ICON)
- Friday, May 13th
  Larry Murphy, Judicial Branch (ICIS, CJIN)

We conducted two-hour meetings with these individuals and asked technical questions about existing systems, current business process, and direction these stakeholders planned for their systems in the future.

In addition, we have conducted follow-up information gathering and telephone interviews with a number of justice practitioners from the State and local levels in Iowa, including Zetta Pilch, regarding the County Attorneys Case Management Project; Tom Becker, the State Public Defender; Lowell Joslin, the Chief of the Law Enforcement Bureau of the Department of Natural Resources; John Gillespie, of the Iowa Telecommunications Enterprise; and Mary Tabor, of the Iowa Office of the Attorney General.

3.1.2 Survey Methodology

To gather information from local level agencies, the MAXIMUS/URL Team created an online. The survey included both technical and business-related questions and allowed respondents to answer either group of questions or both. The survey was distributed to the following respondent groups:

- State Public Defender
- State Department of Natural Resources
- State Attorney General
- Local Judicial Districts (business-questions only)
- County Attorneys
- Law Enforcement Agencies
- Sheriff's Offices Law Enforcement Function
- Sheriff's Offices Jail Function

The survey was distributed from the CJIS Advisory Committee to their respective constituencies on May 9, 2005. Respondents were given until May 25, 2005 to respond to the survey.

In total, there were 127 respondents who completed the survey, categorized by the following respondent groups:

Discipline	Number of Business Section Respondents
Judges	15
Court Clerks	48
Court Administrators	6
Local Police Agencies	20
Local Sheriff Agencies	15
County Attorneys	21
State Public Defender	1
State Attorney General	1
State Department of Natural Resources	0
TOTAL	**127**

The survey was intended as a timely way to reach a broad audience and to elicit information from that audience about general readiness for integration and willingness to

make changes to current business practice to support that transition. The results are meant to be descriptive, but because of mixed response rates among some respondent groups, caution should be taken when generalizing the results.

The business sections of the survey were created to assess the readiness of justice agencies to share information automatically from a business process perspective. It asked general questions about the value behind justice information sharing, as well as specific questions about standardized practices and forms; timely information sharing; security; privacy; and the direction these agencies are heading in the future. The latter categories and their responses, by discipline, are described in detail below.

3.2 As-Is Business Environment

The following section will discuss the current environment by agency at the State level and by discipline at the local level.

3.2.1 Description of Approach

The Business Readiness and the As-Is Business Environment was ascertained through a variety of approaches. The primary mechanism for gathering information from local level agencies (police departments, sheriff's offices, local jails, and local County Attorneys) was the survey. In the business section of the survey, the MAXIMUS/URL Team asked questions that presented scenarios that are current business process challenges in the State of Iowa. The survey questions are listed in Appendix C of this document. The questions sought to determine whether the effort to share the information electronically – mainly changing business processes, current forms, and/or standardizing data elements for collection – was feasible, from the respondent's perspective.

The Business Readiness and As-Is Business Environment was gathered from the State system stakeholders through interviews. The Judicial Branch, Department of Public Safety (DPS), Department of Corrections (DOC), Division of Criminal and Juvenile Justice Planning (CJJP), and the Department of Transportation (DOT) have a significant role in the State exchange process but are also centralized and complex systems with a variety of business goals and constraints.

Information about the Iowa Communications Network (ICN) and Iowa Technology Enterprise (ITE) are presented in the section on the As-Is Technical section.

3.2.2 Judicial Branch

3.2.2.1 State Court Administrator

3.2.2.1.1 Current System Summary

The Iowa Court Information System (ICIS) is the Court case management system and currently supports Court business processes for the Unified Court System in Iowa, which centralized in 1986. The Judicial Branch is in the process of moving to ICIS II, which will maintain the functionality of ICIS but with a state-of-the-art environment. The system is used primarily by clerks to record and retrieve Court event information, and is also used by Court Administrators and Judges. ICIS is case-based and uses a Personal Identification Number (PIN) to identify distinct individuals; the number is not biometrically based or automatically tied to the Department of Public Safety's Division of Criminal Investigation number (DCI#).

In addition to ICIS, the Courts have two other systems on which they rely. The first is the Criminal Justice Information Network (CJIN), which is a system designed to link Court scheduling and case management information with other criminal justice agency information, such as criminal history from DPS, and community based corrections information from DOC. CJIN was developed in an effort to support judges. CJIN established an electronic bulletin board to make appellate opinions available to publishers, the media, and the public and initiated a project pilot testing video conferencing in the 6th Judicial District. In addition, the Courts have the ability to use CJIN to develop/produce Court documents (orders) based upon ICIS data.

The other system is the Iowa Courts Online (ICON), which is a web portal accessing ICIS and makes non-sensitive Court case information available to the public. ICON may be searched by case number or person. Iowa Courts Online also has the capability to provide a secure site for restricted access.

3.2.2.1.2 Current Interfaces and Exchanges

Currently, ICIS exchanges criminal justice information with DOC, DPS, DOT, and CJJP. ICIS also exchanges financial information to the State's Department of Administrative Services. In addition, there have been some successful pilot efforts in the 5th and 6th Judicial Districts that demonstrate the viability of automating Court exchanges between ICIS and local agencies.

ICIS exchanges Court data with the CJJP Justice Data Warehouse (JDW) by transferring the batch data through a standard FTP. CJJP has modeled the database such that it represents data similar to that of ICIS. As such, updating the CJJP JDW database with Court data is a fairly straightforward process.

CJIN provides judges access to Court information along with criminal history, community based corrections and detention status. CJIN data is maintained through daily FTP batch updates from ICIS for Court scheduling and case management information, DPS for Computerized Criminal History (CCH) records; DOC (ICON) for community-based offender data; driver's license information from DOT; and detention information from County Jails.

A transactional exchange exists between the Judicial Branch and DPS and involves the entry of protection orders. Court clerks enter protection orders into ICIS as they are ordered. ICIS, with a real-time exchange, sends the protection order to the Iowa Online Warrants and Articles (IOWA) System by emulating a transaction with the IOWA System's front-end application interface, this appears to the IOWA system as a user directly entering the order. As the exchange goes through the front-end application, the data is submitted to the same validation as if it were in fact entered directly. In addition to passing this information to DPS, ICIS receives an acknowledgement when the protection order has been successfully entered and is also notified from the IOWA System when the protection order has been served. The interface between ICIS and the IOWA System does not require clerk authentication information or workstation identification. In addition, the clerk entering the information is not required to have IOWA System security certification, the ICIS system is considered by DPS as a trusted host or server.

ICIS also receives electronic citations scheduled for a Court appearance from the TraCS system. Citations from local or State law enforcement agencies are uploaded to a file server located at DPS. This transfer is performed daily in an FTP batch format. The Judicial Branch makes a request to DPS and the citations are transferred to ICIS again in an FTP batch transfer. When the case is disposed, the dispositions are sent to DOT's Drivers License System through an FTP batch transfer. The paper citations must still be submitted to the Court, as the electronic transfer does not contain the defendant's signature. TraCS does capture the signature; though it is not currently exchanged with the Judicial Branch.

The Judicial Branch and the DOC co-designed a process for exchanging Pre-Sentence Investigations (PSI), which was facilitated by the CJIS office. The process of designing the exchanges broke down several barriers relating to interpretations of policy, code, Court rule, and practice. Most of the design has been implemented as a batch/transactional exchange. When the Court orders a PSI, the orders are batched overnight to a shared database with the DOC. The DOC retrieves the orders and populates the database with any completed PSIs and other associated data elements (e.g., the PSI writer, date written, etc.). The Judicial Branch is not only able to print the report for distribution, but also posts the PSI to a secure web site for viewing by authorized parties.

From previous exchange analysis projects, the automation of exchanges around warrants was identified as a high priority for integration. Currently, the paper warrant is delivered to the Sheriff for entry into the IOWA System. This creates a burden for the Sheriff's

office. However, in a successful pilot project in Linn County, ICIS sent warrants (the order itself and any recalls) to the Sheriff's warrant system. The Sheriff would enhance or update the order, and if the warrant were served the Sheriff would send a notification through a transaction back to ICIS. Each transaction took approximately 10 seconds. This pilot project demonstrated the feasibility of warrant transactions from the Court, though it is no longer in place since the Sheriff updated his Record Management System.

Another component of the ICIS case management system relates to finance and accounting. ICIS currently sends Accounts Payable voucher data to the Iowa Financial Accounting System (IFAS) for the purpose of printing checks.

Finally, the Judicial Branch must constantly respond to release of information requests from entities outside of the Iowa justice system. The requests are for batch transfers of data, each slightly different from the last. This requires that the ICIS system produce each of these as separate processes. These requests have a considerable impact upon the IT staff and the processing capability of the ICIS system. Currently, the system has a very small window in which additional requests for information can be fulfilled and some requests for information cannot be supported. The Judicial Branch recently discovered that a respected private sector organization was "screen scraping" data from the Iowa Courts Online system to obtain Court information. This activity had a negative impact on ICIS processing for other users of the application and had to be stopped.

3.2.2.1.3 Security and Privacy Issues

Iowa Code and Court Rules guide the Judicial Branch when security or privacy issues are concerned. In general, the ICIS system is open, other than a few protected case types, particularly for juvenile cases. The openness of Court data has put the SCA in the position of responding to the numerous requests for data. The Court also expects case records to be purged or sealed from systems when such an order is issued, especially when the other agencies publish the data.

3.2.2.1.4 Standardized Process and Forms

Although the Unified Court System in Iowa is fully supported by a single case management system, the processes and forms vary from district to district, and judge to judge. In some cases, the Court does not initiate this variance in process; the charging process of the local law enforcement agencies and the County Attorneys initiates some of the differences.

The variance in Court orders is significant, and while some judges appear willing to make changes to their current business process, others are reluctant to abandon their particular way of phrasing an order. The data is consistent as it must be entered into ICIS, but it is the verbiage that accompanies the order (that is currently buried in free text fields) that provides additional meaning and direction would be difficult to capture in an exchange, as it exists now.

3.2.2.1.5 Future Direction

The SCA plans to maintain CJIN and move ICIS to a new platform and front-end application, called ICIS II. ICIS II will provide users with a more robust and state-of-the-art user interface as well as the backend servers. ICIS II should well position the SCA for exchanging information in a service-oriented architecture (SOA) environment.

Areas within the Court are developing standardized processes, primarily in the juvenile arena. However, the majority of adult criminal processes and forms are not expected to change in the near term.

3.2.2.2 Local Court Perspective

In addition to interviewing the State Court Administrator and central ICIS staff, we asked business questions of Court Clerks, Court Administrators, and Judges about Court readiness for interagency information sharing.

3.2.2.2.1 Standardized Processes and Forms

Several of the questions addressed whether agencies saw the benefit of standardized practices and forms as well as readiness to modify or change current business practices to accommodate this standardization. Respondents were asked general questions as to whether customized forms were necessary to agency information processing or a burden, and whether there are adequate staff resources to transition to a standard process. They were also presented scenarios about situations in which information could be improved (adding identifiers to the "Greensheet" and standardizing affidavits and complaint forms among law enforcement) if standardized.

Of the Court respondents (Court Clerks, Court Administrators, and Judges), most agreed that custom forms are not essential, and the implementation of standardization would not be an undue burden. For example, while only 41% of Court Clerks, 50% of Court Administrators, and 30% of Judges thought that customized forms are necessary to practice their role in justice, a majority of all Court respondents did not believe standardized forms would be an intrusion to their current business practice (Court Clerks 86%, Court Administrators 100%, and Judges 60%). This suggests the Court community is receptive to standardization if there is benefit to undertaking the process.

Regarding staffing, respondents were asked about filing with the Courts, and the difference in business practices between small and large jurisdictions, the latter of which County Attorneys typically file, while in smaller jurisdictions, law enforcement may file directly. Respondents were asked whether staff resources would allow a standardization in business practice on this filing issue. Of those who responded, a majority thought that current staffing resources could accommodate a standardized business practice on Court filing. Sixty-two percent of Court Clerks thought there were ample staff resources to implement a standard process, whereas 71% of Court Administrators and 91% of judges thought there to be ample resources.

When asked whether the benefits of standardizing a practice outweighed the need to make a change within a specific jurisdiction's business process, the majority of Court Administrators and Judges thought the benefits of standardization outweigh the investment, while Court Clerks were nearly 50/50 on whether the benefit would be worth the change.

3.2.2.2.2 Timely Information Sharing and Data Integrity

Court personnel had mixed responses in their assessment of whether timely data entry is a barrier to the current business process. Judges were the most optimistic group, with only 30% perceiving the Court Clerks' ability to enter data in a timely fashion as a barrier, while two thirds of responding Court Administrators thought it an obstacle. Court Clerks were nearly a split, with 47% responding that timely data entry is a barrier to the current business process.

When asked how to improve data integrity, Court respondents had several good ideas. Respondents in all three categories (Judges, Court Administrators, and Court Clerks) agreed that moving to standardized processes would help improve both the timeliness and data integrity of information included in current systems. One respondent noted that "standardized forms would result in data integrity and eventually simplify data entry," while another said that the process could be augmented by having "one way, instead of 99" ways of doing business. A common example was the differences in the manner in which Judges currently file orders.

Respondents noted however, that standardization requires some level of enforcement and oversight. One respondent noted that "if customization is to be accomplished efficiently, it must be mandated and complied with. So many times things are directed and not complied with and no one does anything about it." A Court Clerk commented that "an authoritative person would simply need to order this to be done uniformly throughout the State and enforce the policy from the very beginning. If necessary this would include penalties applied."

Court respondents also recognized the importance of common identifiers and how moving in that direction would improve data quality. One judge noted that "a good index to the tracking information would allow better integration. The index should be set up to search both by name and two or three identifying numbers, as well as by sub-jurisdiction." A Court Administrator noted that the process could be improved by "shar(ing) protocols for entering names, identify date of information for last date best info judgments, and provide for optional noticing of specific individuals/cases that enter specific systems."

Court respondents seemed very concerned, however, that improving timely information sharing would have an impact on staffing. Several respondents indicated that current staffing levels would need to be revisited in order to implement business process changes or to comply with new requirements around timely data entry. Many also noted that training should also be improved.

3.2.2.2.3 Security

When asked whether sharing information with other agencies is safe, a majority of Court Clerks and Administrators – 76% and 83% respectively – answered that it is. Judges, however, were more skeptical, only 33% of responding judges thought that trusting another agency with Court data would be safe. When asked whether the responding agency was positioned to adopt the security requirements of another, Court Administrators reported being very willing – 100% responded that their agency would. Seventy-six percent of Court Clerks stated that they would, while 73% of Judges stated that their agencies would be in a position to adopt other security requirements in order to exchange information electronically.

Court respondents had sophisticated ideas about improving information security, beyond user authentication (login and password). Examples include:

- Each agency or entity should be required to have quality control tests in place with regular audits. Use something more than one password, such as two levels of passwords or "fingerprint" passwords. Specific employee confidentiality agreements related to the use of data with training annually on security and confidentiality are also recommended.
- Information sharing will not work unless agencies trust each other to provide accurate data and to safeguard against dissemination of confidential data. Some type of standards would need to be developed with each agency possessing the necessary hardware and software to meet the standards.
- Assigning a security level to each employee, and only allowing employees assigned the highest levels of security to either transmit or receive the confidential information is also a possible option. Perhaps the "lower level" security people could transmit the necessary information to the "higher level" security people, and the information could transmit to another agency once it left "lower level" and reached "higher level" within each agency.
- The agency we are sending information to should have the same confidentially rules as the Court has. There should be a computer program that would allow us to transfer information to other agencies by a new screen so clerks can be sure the information in complete and a "send" button like we have for the District Attorney registry.
- Statutory requirements for encryption of confidential data before electronic transmission must be considered. Statutory standards need to be met for protection of the transmission systems from outside hacking or breaches. Regular security audits should be required from all participants in the system, with one agency (perhaps the Attorney General's office) authorized to monitor compliance.

3.2.2.2.4 Privacy

For the most part, Court respondents indicated that they would not use victim and perpetrator information outside of the normal process of managing a Court case (i.e., for notification purposes). Almost 70% of Court Clerks and Judges (68% and 69%, respectively) stated they would not use the information, while only 50% of Court Administrators reported that they would use it.

When asked how they would use this sensitive information, Court respondents overwhelmingly indicated that they would defer to the current policies around confidentiality that they currently follow, using security levels in ICIS and setting them appropriately. One respondent noted that "ICIS II has confidentiality limits so the public would not necessarily have access to this information. It would need to be handled through ICIS."

With regard to making juvenile information more readily available to the justice system at large, Court respondents were mixed. Approximately one half of Court Clerk and Court Administrator respondents thought that the increased availability of information such as diversion and informal adjustment would be beneficial if made more broadly available. However, only 33% of Judges thought this information would be useful to other agencies in the justice enterprise.

3.2.3 Department of Corrections

3.2.3.1 Current System Summary

The Iowa Department of Corrections (DOC) has over 38,000 offenders under supervision. Approximately 9,000 offenders are in prison and 28,400 in community-based corrections. The DOC is responsible for nine prisons and eight community-based corrections districts. The DOC is supported by the Iowa Corrections Offender Network (ICON) as their management information system. The services provided by ICON include medical, pharmacy, commissary, inmate banking, and an offender management system. The offender management system contains offender demographics, criminal and corrections supervision services history, assessment, criminogenic needs and interventions, rules, rule violations and hearings, housing information, warrants, and detainers.

Within the offender demographics, ICON contains:

- Personal Information
    - Name and aliases
    - FBI/DCI numbers
    - Physical characteristics
    - Address and phone number
    - Body markings and threat groups

- Family, associate, and enemy information
- Employment history
- Birth and citizenship information
- Financial history

The assessment information developed and retained in ICON is, in part, produced by the Courts. The Pre-Trial Investigation and the Pre-Sentence Investigation (PSI) are significant assessments that assist the Court in making critical decisions around pre-trial supervision and sentencing. ICON is accessed through a secure network; however the DOC makes ICON information available through a variety of mechanisms, including a public access site that provides name, DOC number, offense, age, sex, location information, and significant dates including tentative discharge date.

3.2.3.2 Current Interfaces and Exchanges

Currently, DOC exchanges information with the Judicial Branch (Criminal Justice Information Network, or CJIN) and (Iowa Courts Information System, or ICIS), Department of Public Safety (Kaleidoscope), and The Division of Criminal and Juvenile Justice Planning (Justice Data Warehouse, or JDW). The CJIN, Kaleidoscope, and JDW exchanges are all FTP batch transfers conducted on a regular basis. The transfer to CJIN populates the CJIN database with updated information on offenders who are in community-based corrections. This exchange allows the CJIN users, primarily judges, the ability to view this information in conjunction with offender information from other justice agencies. The batch transfer to Kaleidoscope populates the database with information on offenders who are in community-based corrections. This exchange allows law enforcement to view this information through the DPS network. The batch transfer to the JDW is translated by CJJP using a fairly complicated algorithm to match the DOC offenders with Court data, and a number of other data sources. The CJJP maintains the Court data representations requiring the translations from DOC data. CJJP uses the data for research and legislative requests for analysis.

The DOC and the Judicial Branch co-designed a process for exchanging the PSI, which was facilitated by the CJIS office. The process of designing the exchanges broke down several barriers relating to interpretations of policy, code, and practice. Most of the design has been implemented as a batch/transactional exchange. When the Court orders a PSI, the orders are batched over nightly to a shared database with the DOC. The DOC retrieves the orders and populates the database with any completed Pre-Sentence Investigations and other associated data elements (e.g., the PSI writer, date written, etc.). Judicial is not only able to print the report for distribution but has the PSI posted to a secure web site for viewing by authorized parties.

3.2.3.3 Standardized Processes and Forms

The DOC uses standardized forms and reports, and most of these are through ICON. The PSI is an example of a form developed through an application on ICON. Although the

data in the PSI is locked in a PDF document, the document is standardized throughout the State. As mentioned above, the process of exchanging PSI between community-based corrections and the Courts was recently standardized, demonstrating the ability and willingness to take on a complicated business process. Most of the other forms that the DOC produces are for internal use, but a major exception is the Pre-Trial Investigation for use by the Courts. This report is ordered frequently by the Court with an expected relatively short turnaround. It is currently exchanged through the paper process.

3.2.3.4 Security and Privacy

ICON has a separate security application for ICON user accounts, passwords, and levels of access. The DOC has also made available to law enforcement a limited version of ICON via the web. In addition, to law enforcement access, the DOC has provided limited offender data to the public via the web. These limited databases are outside of the Department's DMZ.

3.2.3.5 Future Direction

The DOC is anticipating an exchange with the Judicial Branch in which ICIS would exchange charges and sentences on offenders placed in the custody of the DOC. This exchange is still in the planning phase; as of yet there is no date for when this is expected to occur. The DOC is also anticipating an exchange with the DPS (Kaleidoscope) where the DOC would provide information on offender movement and sex offender-related information. Currently this exchange is considered outside of scope for Kaleidoscope.

Although the DOC uses FTP for most of the current exchanges with other justice agencies, they express a strong agreement that SOA based standards should be considered for any future integration framework, including the use of XML and GJXDM-conformant schemas.

The DOC direction with ICON does not seem likely to change in the near-term, short of continued enhancements.

3.2.4 Attorney General

3.2.4.1 Current System Summary

The Iowa Attorney General's office is heavily involved in several aspects of the Iowa criminal and juvenile justice processes. Forefront among these is the prosecution of serious felonies and the preserving of convictions and sentences won by the County Attorneys. Information concerning the current technical environment of the Attorney General's office was obtained using a survey tool available via the Internet. The information is fairly abbreviated, but provides a good baseline of where the agency is in its current technology life-cycle. Maintenance of the environment is provided by a small staff of one or two resources.

Since the Attorney General's Office tries appellate cases, it is seldom the originator of information within the justice enterprise. The office currently benefits from the availability of court information through Iowa Courts Online and could envision the sharing of information with County Attorneys once its common case management initiative is operational.

3.2.4.2 Standardized Processes and Forms

From the Attorney General's office perspective, the burden of standardizing around a single Court filing process may not be worth the effort. The respondent thought that there would not likely be adequate staffing resources to require a standard process, and that direct filing with the Court would likely impact the ability of the County Attorney to file charges they think best.

3.2.4.3 Timely Information Sharing

When asked whether timely data entry is a barrier to the current exchange, the Attorney General's office answered "yes," mostly due to the current shortage in staffing that many local jurisdictions are facing in Iowa.

3.2.4.4 Security and Data Integrity

When asked whether information sharing with other agencies is safe, the Attorney General's office responded no. When asked what could be done to improve security around interagency exchanges, the respondent stated that implementing levels of access determined by need to know as well as understanding what agencies accessing information and for what purposes would be important first steps.

3.2.4.5 Privacy

The Attorney General respondent reports that its agency already uses victim and perpetrator information, but that data in a separate module within their case management system. Since the Attorney General's office tries appellate cases, there are some instances in which victim notification must be done. In those instances, the Attorney General typically turns to the County Attorney who originated the case, as they have the formal responsibility for notification as well as the appropriate victim information. A recent bill passed by the legislature that would automate victim notification might affect this process in the future.

The respondent did not feel that the release of juvenile related information, such as dispositions or informal adjustments, would benefit other justice agencies.

3.2.5 Department of Public Safety

3.2.5.1 Current System Summary

The Iowa Department of Public Safety (DPS) manages key information systems for the State's law enforcement community through the Iowa On-line Warrants and Articles

(IOWA) system. A State switch provides law enforcement agencies around the State access to the State's criminal history repository and the IOWA system database, which contains what is commonly referred to as "hot files", (e.g., warrants, protection orders, sex offender registry, stolen vehicles, stolen articles, and guns). In addition, the switch provides other key information to local, state, and federal criminal justice agencies throughout Iowa, such as motor vehicle registration; driver license; master name indexes with associated criminal history records, and administrative messages (law enforcement e-mail). The switch also serves as a link to the national law enforcement network National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (NLETS).

In addition to the State switch and associated systems, DPS provides law enforcement access to Kaleidoscope. Kaleidoscope provides valuable and timely information sharing regarding offenders who have been released into community-based supervision programs managed by the DOC, and those detained and/or released pending trial from the Polk County Sheriff's Detention facility. During routine traffic stops, law enforcement officers are notified of an individual's status as a probationer or person awaiting trial. Officers are notified of the Probation Parole Officer (PPO) name, phone number, and e-mail address should they need to contact them to continue their investigation.

DPS also manages the State's automated fingerprint identification system (AFIS), which began to gather information through Livescan transfers in the early 1990s. The growing number of fingerprints being transferred electronically to AFIS not only improves the quality and timeliness of the prints, but also facilitates the creation of an arrest record in the CCH and a positive identification reflected in the assignment of a DCI#, which is available to other State agencies.

3.2.5.2 Current Interfaces and Exchanges

Currently, DPS (through the CCH and the IOWA System) conducts two primary exchanges with the Judicial Branch's ICIS System on Dispositions and Orders of Protection. Dispositions are transmitted to DPS by FTPs in a batch once a day via a trusted connection. The dispositions are matched to an arrest through the Document Tracking Number (DTN). If there is a match, the criminal history record is updated. If there is no match, the update is rejected. The DTN is initially generated at the time of arrest (fingerprinting). The arrest creates an incident and DPS receives this information through the fingerprinting process. Law Enforcement moves this information to the "Greensheet" which is then used to pass charge and disposition through County Attorneys to the Courts. This form contains personal identifiers such as name, demographics, DOB, a Document Tracking Number (DTN) and the arrest charges. The Greensheet may also contain a Division of Criminal Investigation Number (DCI#), FBI#, and SSN if known. There is no terminal or user authentication for the Judicial Branch clerks originally entering this information, beyond signing on to ICIS, their system of record.

Orders of Protections, however, are real-time transactions, which look like a an ICIS entry to the Court clerks, but in the background transmit all the data elements required by the IOWA System for entering orders of protection. The data is sent to DPS emulating an IOWA System protection order entry. From this transaction, the DPS knows the jurisdiction and the Court entering the information in the system, but not the individual clerk. In other words, Court clerks have not had to meet the IOWA System security requirements or NCIC regulations in order for this transaction to occur. This exchange also provides information back to the Courts. If an individual is served with the order of protection, the IOWA System sends this information back to ICIS. In addition, when a protection order is received into the IOWA System from the Courts, the entry is acknowledged with a message back to ICIS and a broadcast message is sent to the local law enforcement agency, indicating if it is a mandatory arrest. The local law enforcement agency can "enhance" the record at this time.

In addition to these primary transactions with the Courts, the Kaleidoscope project receives batch FTP transfers from DOC (ICON) and the Polk County Jail Management System on a nightly basis, providing community based corrections, and other placement information to law enforcement. Kaleidoscope also originally provided probation notification back to the PPO via e-mail, however, but that functionality has been disabled because of the inability to provide very detailed information about the subject, the nature of the law enforcement query, and the officer involved. Another major factor was that cover investigations on the subject at hand may be jeopardized by the unknown notification to the PPO and potential tip-off to the subject. Currently DPS is establishing 10 seats for this program and will make the information available through a portal.

The DOT maintains vehicle registration and reciprocity information. Both of these systems use web-services to exchange data with DPS in the form of Open FOX Markup Language (OFML). OFL is not the standard that the justice community currently uses nor is it conformant with GJXDM. However, this is one of the few web-services exchanges in justice and demonstrates a readiness on the part of DPS to consume data through web-services.

3.2.5.3 Standardized Processes and Forms

DPS primarily relies on automation through file transfers, queries, and data entry. Forms are primarily screen-based. With regard to entry into the IOWA System, entry of Hotfile and CCH Data is bound by NCIC and IOWA System Rules and Regulations. Collecting standardized information on protection orders in a standard format – it appears like an ICIS screen to Court Clerks – is in large part the reason why this exchange has been so successful.

3.2.5.4 Security and Privacy

Access to the IOWA system is bound by NCIC certification and IOWA System Rules and Regulations, which made the initial interfaces with the Courts intricate at first. This security restriction also precludes Judicial Branch staff from the ability to see information

they have entered (once it has been uploaded to the IOWA System) and/or make changes. When there are errors, and when a Court clerk enters then invalidates a record on the same day, DPS must invalidate it manually. While cumbersome, the overall exchange between the Courts and DPS on both dispositions and protection orders has passed an NCIC audit.

3.2.5.5 Future Direction

In addition to the Kaleidoscope effort, there are other exchanges that DPS has considered automating, such as sending arrest records (with DCI# and other demographic information) to ICIS. AFIS transactions are electronically sent to DPS, but there is no exchange between AFIS and the CCH. Although DPS sees this as the exchange with ICIS as a potential benefit, the business issues currently have not been examined.

Although warrants, like protection orders, are entered into both ICIS and the IOWA System, DPS is not comfortable automating this transaction. Currently, the warrants are entered by the Sheriff directly into the IOWA system. There are several reasons why a warrant exchange between the Courts and DPS is currently not feasible. First, the data entered into ICIS does not meet NCIC requirements; there is the need for Sheriff Offices to enhance the record and perform quality control checks on the information. A second reason is that the transaction would need to be real-time to ensure the accuracy of the warrant information. Currently, Sheriffs are required to do an IOWA system check prior to serving a warrant to ensure it is still valid. Because it is associated with an arrest, there are significant concerns about civil rights and false arrest issues arising if accurate information is not available.

3.2.6 Department of Transportation

3.2.6.1 Current System Summary

The Traffic and Criminal Software (TraCS) system is an initiative administered by the DOT that allows law enforcement agencies to send information – Accident Reports, Electronic Citation Component (ECCO), Operating While Intoxicated (OWI) complaints, and Incident reports – to the Department of Transportation, the Judicial Branch, and their local RMS. The traffic citation is passed to the Judicial Branch case management system through DPS. For most law enforcement agencies the reports are created in the car and hard copies made available instantly.

Currently, 160 law enforcement agencies in Iowa use TraCS, and they expect to add another 40 this summer. TraCS evolved in such a manner that the State of Iowa owns the source code and as such, makes the program available to other jurisdictions for use. This ownership of the source code allows jurisdictions to use an easily adaptable Software Development Kit (SDK) to install TraCS and modify forms and data fields. This makes TraCS easy to replicate. Currently, 22 states are using TraCS.

TraCS is a very versatile product with rich functionality. The DOT reports that some smaller law enforcement agencies in Iowa use it as a Records Management System. Benefits of TraCS include increased officer efficiency and the availability of more accurate criminal and traffic data.

3.2.6.2 Current Interfaces and Exchanges

Currently, information is transmitted from TraCS to DPS via the IOWA System. The process is based on an FTP process currently. This information is then sent from DPS to ICIS. This information is transmitted to DPS via XML. Currently, there is no acknowledgement from either ICIS or DPS that the information that DOT submitted through TraCS has been received.

There is an exchange between TraCS and ICIS currently on traffic violations with appearances. The information is initially passed (via FTP) to a file server at DPS from where it is retrieved by ICIS. The citation populates ICIS, however, the Court still requires the paper citation as the official filing document. Specifically, the Court requires the defendant's signature associated with the any traffic citation. TraCS captures the signature image of both the officer and the defendant but this is not a part of the information exchanged.

TraCS exchanges information with many local RMS systems; in some instances the TraCS data is extracted and transferred as XML. However, not all local RMS systems are able to accept XML exchanges. For example, Cedar Rapids and Des Moines Police Departments use Intergraph, which is XML compliant and can interface directly with TraCS. Currently, the Des Moines Police Department is redoing all of its mission critical systems (RMS, CAD, Mobile) and has required them to write the XML interface with TraCS. With Sleuth, a product used by many small agencies in Iowa, the State paid for the interface, and then they gave it to the local police departments.

3.2.6.3 Standardized Processes and Forms

The use of TraCS has helped encourage the creation of common forms and data elements on key law enforcement forms. Initial TraCS implementation in Iowa automated the uniform crash report and the uniform traffic citation. Recently, TraCS has developed a common criminal incident report, which is NIBRS compliant. The State has also come to common agreement on the OWI complaint form which is supported by TraCS, with most of the State (except for Polk County) using the form. These common forms and collected data elements will undoubtedly better position local law enforcement to participate in statewide information sharing.

3.2.6.4 Security and Privacy

The Driver's License, Vehicle Registration, and TraCS systems all rely on username/password authentication at their fundamental level of security. While TraCS

utilizes a DPS file server as the central location for distributing its various reports to the Courts, it is not considered in the same context as an NCIC/NLETS terminal connection and consequently, no location, terminal, or user information is included with the files. As such, it is not subject to the same stringent security policies.

3.2.6.5 Future Direction

TraCS has extensive plans for the future. In addition to the 40 Iowa law enforcement agencies it plans to bring online later this summer, they are working on transmitting information to the DPS Kaleidoscope pilot initiative in Polk County. They are currently about to change how to transmit citations to move to a more transactional approach to move data using XML to a database at DPS, rather than a file transfer to a flat file server. There have also been discussions with the Judicial Branch to enable true e-filing using XML.

3.2.7 Public Defender

3.2.7.1 Current System Summary

The State Public Defender's office is located in Des Moines and provides services to all 99 Iowa counties. The State Public Defender coordinates provision of legal representation to indigent persons under arrest or charged with a crime, in juvenile cases, and on appeal in criminal and post-conviction relief cases. This legal representation is provided through State Public Defender Offices or through private attorneys who contract with the State Public Defender, or attorney appointed by the Court.

The Public Defenders office is currently utilizing a custom-built application for the handling of their case management; however, the deployment of the system is decentralized and there is no central database for Public Defender information (although they do share a common e-mail server). All Public Defender offices have their own localized databases because of the strict privilege restrictions around the sharing of Public Defender information in Iowa.

Because of the strict information sharing requirements, the State Public Defender does not expect that the defender information systems will be directly integrated with any other as a result of the CJIS planning effort. Rather, he perceives his role on the CJIS Advisory Committee to protect Public Defender privileges and prevent integration of information that should not be shared and ensure Public Defender access to information that is publicly held and/or appropriate for Public Defenders' access.

3.2.7.2 Standardized Processes and Forms

With regard to customized forms, the Public Defender's office indicated that, generally, standardized processes are essential to current business practice, and that he did not

perceive any possible future efforts to customize forms or normalize business processes to accommodate a statewide integration effort to be a burden.

However, when asked about direct filing with the Courts, and the difference in business practices between small and large jurisdictions (the latter of which County Attorneys typically file, while in smaller jurisdictions, law enforcement may file directly), the Public Defender's office responded that while current staffing structures would likely accommodate this direct filing, moving toward a standardized process would likely affect the agency's ability to file the charges they think most appropriate.

When asked whether the benefits of standardizing a practice outweighed the need to make a change within a specific jurisdiction's business process, the State Public Defender did not believe so in this circumstance.

3.2.7.3 Timely Information Sharing, Data Integrity

The Public Defender's office indicated that timely information sharing is a barrier to the current business process. Timely information sharing, he noted, is not pervasive but is county dependant, based on circumstances and culture of each county.

3.2.7.4 Security

In Iowa, sharing defendant information with other agencies is not applicable. According to the respondent, public defender field office databases contain legally privileged information that may not be lawfully shared with anyone outside that field office – not even other public defender offices or the State Public Defender Office. So, for public defender data, no sharing can be permitted.

3.2.7.5 Privacy

The survey question regarding whether information about victims or defendant release would be used is not applicable to the Public Defender. In addition, the respondent noted that his office would likely not use juvenile adjustment information.

3.2.8 Division of Criminal and Juvenile Justice Planning

3.2.8.1 Current System Summary

The Iowa Division of Criminal and Juvenile Justice Planning (CJJP) manages and maintains Iowa's Justice Data Warehouse (JDW). The JDW was created in 1998 to provide "one stop shopping" for criminal and juvenile justice statistics to the Iowa Legislature, Executive Branch, and other policymakers. Currently, information from the Iowa Judicial Branch case management system (ICIS) as well as the Department of Corrections ICON system is uploaded in flat files to the JDW on a monthly basis. The JDW does not receive all ICIS and ICON data; rather it extracts data elements that have been commonly agreed-upon by involved agencies.

The JDW also receives information from the Polk County Jail Management System and the State Departments of Human Services and Public Health on an ad hoc basis.

The JDW is a component of an enterprise-wide data warehouse (EDW) for the State of Iowa. The EDW involves a partnership with CJJP, Department of Corrections (DOC), Judicial Branch, the Department of Revenue and the Department of Human Services. The EDW is housed in the Department of Administrative Services-Information Technology Enterprise (DAS-ITE). ITE provides staff support and assistance with the Teradata platform and the NT staging and Business Objects servers. They may assist with the monthly data loads extract, transform, and load (ETL) scripts, load stats, etc.), provide maintenance to hardware and software, and do monthly data backups. While statewide support for the data warehouse has remained stable, the EDW has the capacity for expanded use.

The JDW is maintained in CJJP because it is considered a neutral site; CJJP does not represent any one justice agency but rather the system overall. For this same reason, CJJP and the JDW may play an increased role in a statewide CJIS integration effort. The CJJP Administrator understands that there may need to be changes to the organizational structure, if necessary, to accommodate the CJIS effort within. Currently, the CJJP is directed by an oversight body made up of judicial, executive, legislative members, and local officials and community agency members.

3.2.8.2 Current Interfaces and Exchanges

Data from ICIS and ICON are uploaded to the JDW through batch file updates on a monthly basis. The JDW is able to consume ICIS data without much translation, as the data warehouse was somewhat based upon ICIS standards as ICIS was in place prior to the development of the JDW.

The ICON system was developed after the JDW, and as such, requires significant translation. The ETL between ICON and the JDW takes several hours. Currently, the Department of Corrections does not maintain a common identifier to facilitate linking between its data and the Court information; currently that linking is managed by a series of complex algorithms maintained by the DAS-ITE.

Corrections data from ICON and Judicial data from ICIS are kept separate and distinct during their respective loads. These two collections of data are later correlated against each other after the load using a series of algorithms to match DOC's individual-based data with the Judicial Branch's case-based data. Common identifiers are used as the parameters for the algorithms, and an average 92% hit ratio is currently achieved.

The JDW is updated periodically (as needed) from the Department of Public Health. Additionally, the Department of Human Services and the Department of Revenue update the EDW on a regular basis. The Department of Public Health provides Substance Abuse Program information, while the Department of Human Services provides access to Child

Welfare data sets. Other agencies (e.g., Department of Homeland Security, County Attorneys, DOT.) have also approached CJJP for inclusion in the JDW.

3.2.8.3 Standardized Processes and Forms

Since CJJP maintains the data warehouse and is not directly involved in the administration of justice, the challenges associated with implementing real-time justice information sharing in Iowa (common data fields and transmission abilities) are not directly relevant to CJJP this aspect of CJJP's responsibilities.

However, it is abundantly clear that for agencies that intend to upload data to the data warehouse that common data representation facilitates the process. For example, an effort began about four years ago to standardize data collection in the Juvenile Court Services, and since then the ICIS juvenile data has improved significantly in the past three years. CJJP also has been assisting the Courts on developing a common intake and assessment form for juvenile intake, which will be implemented in ICIS in the next two months. Standardizing the data collection process helps improve the overall quality of data being uploaded to the JDW, and also would further justice information sharing between agencies.

CJJP staff is interested in learning more about XML and how the Global Justice XML Data Model could be used to foster the exchange of information from other agencies using standardized formats. The use of XML decouples CJJP data fields from those of the sending agencies, and could assist in receiving the data. CJJP acknowledges it would need to work to determine the feasibility of consuming XML formatted data.

3.2.8.4 Security and Data Integrity

The JDW is not available to external entities for specific case or individual information. The data integrity is dependant on the entities providing the data. CJJP must match the data from the various sources as best they can to not represent cases or persons as being the same across systems when they are in fact not.

The JDW is designed for the purpose of producing aggregate reports, statistics, and analysis. Only this information is released. Should the JDW be made available to query specific offender data the issues of security and data integrity would require additional consideration.

3.2.8.5 Future Direction

In Iowa, there is a movement to better share information about convicted sex offenders and their whereabouts among local justice agencies and practitioners. The Iowa Legislature has passed legislation that requires CJJP to conduct a comprehensive study about sex offenders, including how technology could assist in their tracking and

management. The bill requires that CJJP staff the Task Force to oversee the study and requires it to make recommendations about how to use the data from other state agency systems to better track addresses for sex offenders.

In addition to the above, one of CJJP's interests in CJIS is to improve criminal justice planning and administration and to continue to position itself as a resource to other justice agencies. From their perspective, the more integrated that justice data systems are, the easier it is for the JDW to extract good information for management as well as research and statistics.

CJJP also has several initiatives that have the potential of adding to the capabilities of the JDW. These include the County Attorney Case Management Project, the OWI tracking grant involving the DOT, and project Kaleidoscope which involves DPS, DOC, DOT, and the Polk County Sheriff's Office.

3.2.9 Department of Natural Resources

The Iowa Department of Natural Resources (DNR) has law enforcement authority and focuses on fish and game enforcement, as well as motor vehicle issues for boats, snowmobiles, and ATVs. Its Law Enforcement Bureau (LEB) has the mission to protect the State's natural resources, to provide public safety, and to educate and serve the public. The DNR has 81 officers operating in all 99 of Iowa's counties at the present time.

Currently, the DNR does not have a centralized system for writing citations. The Chief of the DNR recently purchased laptops that officers can use to generate motor vehicle citations and other law enforcement documents, which are transmitted directly (e-mail or paper) to the Clerk of Court in that jurisdiction. The DNR also hopes to transition to using TraCS as their system of record and to generate electronic citations via the laptops.

In addition to transitioning to TraCS, there are some DNR officers who use Cyberlinks, which is a web-based system managed by DPS that allows subscribers to view drivers license and motor vehicle information. DNR currently pays for a limited number of seats to access this information.

Overall, DNR is eager to move to TraCS and expand its ability to participate in justice information sharing.

3.2.10 County Attorney

3.2.10.1 Current System Summary

The breadth of different technical environments among Iowa's County Attorney offices is significant. The differences can typically be drawn between the rural and urban areas. Of the 99 offices, 49 of them are still served by a part-time County Attorney. In previous studies, the lack of automation in the County Attorney offices was cited as a major barrier to the ability of Iowa to achieve statewide integration.

Since that report, the County Attorneys have worked toward removing that barrier by creating the Iowa County Attorneys Case Management Project. This pilot effort has as its goal to provide a common prosecutor case management system to any Iowa County Attorney's office that chooses to participate. Two different applications are being made available through the project: ProLaw from Thompson Elite and Judicial Dialogue from Judicial Dialogue Systems. The number of participants has fluctuated over the course of the effort, but at the time of this writing, 13 counties were prepared to test and implement one of these two solutions by July 1, 2005. However, other counties may still join the effort, as it is expected that an early success of the project will encourage broader participation. Another County Attorney office is also expected to be implementing in the near future, but not in the initial rollout of the application.

3.2.10.2 Standardized Processes and Forms

County Attorney respondents indicated a willingness to move to standardized forms and practice to support a CJIS initiative. While only 41% of County Attorneys who responded indicated that standardized forms were essential to their current business practices, 77% responded that the effort to standardize would not be an intrusion, if the outcome meant systemwide information sharing.

Respondents were somewhat mixed when asked whether a standardized Court filing process is a good idea and if it can be sustained at current staffing levels. Forty-three percent of respondents reported that current staffing is adequate to support that effort, while the remaining respondents indicated that there was not adequate staff in their agencies to support a change in the filing process. While 65% stated that they did not feel that moving to this standardized process would affect their ability to file charges as they think best, that same 65% indicated the effort to move to a standardize process for filing would likely not be worth the change.

3.2.10.3 Timely Information Sharing and Data Integrity

Respondents were nearly split when asked whether timely data entry is a barrier to their current business process. Forty-five percent of respondents indicated that timely information entry is a barrier to current process, while the remaining 55% indicated that it is not.

When asked what could be done to improve timeliness and data integrity, many County Attorney respondents noted that standardizing forms would be of assistance. One respondent noted, however, the importance of ensuring that information currently collected on these forms is relevant: "The problem with utilizing standardized forms is that they are often confusing, particularly for defendants and their attorney, and some standardized forms already in use are not user friendly."

3.2.10.4 Security

The County Attorneys, generally speaking, are confident with their current security protocols and willingness to adopt a certain security standard in furtherance of statewide justice integration. Specifically, 76% of respondents reported that they perceive that sharing information with other agencies is safe, and the same number reported that they are willing to adopt new security policies to participate in integrated justice efforts.

In addition to user authentication, County Attorney respondents suggested that both formal and informal relationships, as well as professional guarantees, with agencies with which information sharing is taking place can foster security.

3.2.10.5 Privacy

When asked whether they would make use of electronic release information about victims and perpetrators, 86% stated that they would, which may reflect the County Attorneys' role in Iowa around victim notification. When asked how they would manage that information, they indicated overwhelmingly that they would rely on the current protocols, rules, and statutes in place around confidentiality of information.

A couple of respondents made note of the importance of keeping victim information confidential and stated that "I would limit the amount of victim information if any at all. If you were to put registered victims in the system for notification purposes, it would have to be strictly protected for safety."

In addition, a majority of County Attorneys indicated that they would benefit from increased availability of juvenile system information: 76% of respondents stated that they would make use of information about County Prosecutor Diversion and Juvenile Informal Adjustments, as examples.

3.2.11 Sheriff Offices

3.2.11.1 Current System Summary

There are 99 Sheriff Offices in the State of Iowa – one in each county. A survey to gather information from this geographically dispersed group was developed and made available via an Internet web site. All 99 Sheriff Offices were invited to participate in the information gathering process. Of those reporting the use of Records Management

Systems and Jail Management Systems, they reported using a wide variety of solutions from different vendors.

3.2.11.2 Standardized Processes and Forms

When asked whether the Greensheet be eliminated and key charging identifiers - Document Tracking Number (DTN), a DCI#, FBI#, or Social Security Number – be included on charging documents, the majority of respondents said that it would not be difficult to include identifiers on these forms – only one respondent thought it would be very difficult to include this information.

Like the Courts, while Sheriffs do not necessarily believe standardized forms are required to conduct current business practice, they do not think of standardization as an intrusion. Only 42% of respondents said standardized forms were critical to current business practice, but 100% of Sheriff respondents agreed that moving to a standardized form would not be an intrusion.

While Sheriff agency respondents were concerned with the staffing impacts of shifting to a standardized Court filing process, they seemed to feel that the standardization would not negatively impact the justice process and that the "costs" associated with moving to standardization would be outweighed by the benefits of information sharing. Specifically, 66% of respondents thought there would be staffing impacts in moving toward a standardized Court filing process. However, 83% reported that a standardized process would negatively affect the Court filing process and 66% indicated that the benefits of standardizing around this process would outweigh the burdens of implementing a business process change.

3.2.11.3 Timely Information Sharing and Data Integrity

For the most part, Sheriff agencies seem content with the current timeliness of data entry: only 17% of respondents indicated that it was a problem in the current business process.

When asked what could be done to improve data integrity, Sheriff respondents noted that customized forms and processes would be beneficial. One Sheriff's Office noted that "standardized forms and data submission would simplify the process and possible eliminate errors," while another commented that "standardization of forms would be beneficial. The problem would be to get everyone on the same page. As it exists now, there are various breakdowns between law enforcement, prosecuting attorneys, and the Courts."

In addition to standardizing, Sheriffs also recommended "interlinking area agencies with information sharing access."

3.2.11.4 Security

Most Sheriff agencies – 80% of survey respondents – were confident that sharing information electronically with other agencies is secure. In additional, all survey respondents indicated that their agency would be willing to adopt the security policies of another agency in order to facilitate cross-agency information sharing.

Respondents had several good ideas around ensuring information security, such as:

- Encryption, ownership of the information, and authentication.
- Restricting individuals that could receive information, unless the information was necessary for officer safety
- Firewalls
- Established policies and procedures among agencies that are sharing information
- Using security systems, such as bio-key, where only truly authorized persons can access secure files
- Audit trails of the information and possibly biometric access to identify those situations where it becomes a problem
- 28E agreements
- Electronic tracking of the dissemination of information as to who accessed what and when

3.2.11.5 Privacy

Sheriff respondents overwhelmingly indicated that they would make use of defendant release information as well as information about youth involved with the juvenile justice system. Ninety percent of respondents stated that they would use victim and perpetrator information if it was made available them electronically.

When asked how they would manage that information, Sheriff respondents stated that they would rely on current statute and policy to guide them. One respondent, however, added that "…I do think we would need some help from the legislature as there is quite a bit of information that currently under the Open records law allows people to view all types of data within our systems."

One hundred percent stated that they would benefit from having more information about juveniles who had participated in diversion or other informal adjustment programs.

3.2.12 Local Police Agencies

3.2.12.1 Current System Summary

There are 383 local law enforcement agencies in the State of Iowa. Of those agencies, e-mails containing information about the survey were sent to the 161 with e-mail addresses registered at the Iowa Law Enforcement Training Academy. Of those reporting the use

of Records Management Systems, respondents reported using a wide variety of solutions from different vendors.

3.2.12.2 Standardized Processes and Forms

When asked whether the Greensheet be eliminated and key charging identifiers – Document Tracking Number (DTN), a DCI#, FBI#, or Social Security Number – be included on charging documents, the majority of respondents said that it would not be difficult to include identifiers on these forms. Only one respondent thought it would be very difficult to include this information.

Like the Courts, while local law enforcement agencies do not necessarily believe standardized forms are required to conduct current business practice, they do not think of standardization as an intrusion. Only about half of respondents said standardized forms were critical to current business practice, but 100% of police department respondents agreed that moving to a standardized form would not be an intrusion.

While local law enforcement respondents were concerned with the staffing impacts of shifting to a standardized Court filing process, they indicated that the standardization would not negatively impact the justice process and that the "costs" associated with moving to standardization would be outweighed by the benefits of information sharing. Specifically, 60% of respondents reported there would be staffing impacts in moving toward a standardized Court filing process. However, 80% reported that a standardized process would negatively affect the Court filing process and 60% that the benefits of standardizing around this process would outweigh the burdens of implementing a business process change.

3.2.12.3 Timely Information Sharing and Data Integrity

For the most part, local law enforcement agencies seem content with the current timeliness of data entry: only 24% of respondents indicated that it was a problem in the current business process.

When asked what could be done to improve data integrity, police responses focused on improved training. One respondent noted that "standardized training from Basic Academy on with standard business practices would improve data integrity greatly," while another noted that "additional data integrity training for data entry personnel" would improve data quality.

That said, law enforcement respondents also had concerns about staffing in this regard. Comments include: "budgeting for data entry personnel would be my only question mark," "no funds to support the system suggested," and "we would need to hire secretary or administrative person to do data entry."

3.2.12.4 Security

Local law enforcement respondents overwhelmingly believed in information security; 100% of the respondents believed that sharing information electronically was safe. When asked if they would adopt another agency's security policy in order to share information, nearly 90% of them said that they would.

When asked what can be done to facilitate improved information security, police responses focused in three areas: user authentication, the creation of common security protocols and interagency agreements, and strong training on security policies and procedures. Respondents note that "they would definitely have to be some very strict guidelines surrounding the exchange of information, and proper training in the use" of security protocols and policies. Another respondent suggested implementing "written agreement(s) accepting liability and potential criminal prosecution for improper use" of information.

3.2.12.5 Privacy

Local law enforcement respondents overwhelmingly indicated that they would make use of defendant release information as well as information about youth involved with the juvenile justice system. Nearly 90% of respondents stated that they would use victim and perpetrator information if it was made available to them electronically. Most of the comments indicated that usage of this information would be driven "by using written policies and training, the same way we handle all other confidential information," and "by following our policies and procedures as it pertains to confidentiality." Another noted that the information would be useful for law enforcement, remarking that "it would be released to the victim and posted on our internal bulletin board for officers, (but) not accessible by the public."

When asked whether information about juveniles who had participated in diversion or other informal adjustment programs would be beneficial, 84% stated that they would benefit from having more information of this nature.

3.2.13 Enterprise View

Currently, there are important state-to-state exchanges that are taking place that demonstrate Iowa's ability to and interest in exchanging information electronically between agencies. While most of these exchanges happen via FTP, the exchange between DPS and the Courts on protection orders demonstrates significant promise in that they occur on a real-time basis. In addition, the interface, while laborious to create, is compliant with the strict DPS security regulations necessary to maintain NCIC certification and IOWA System Rules and Regulations. In addition, the State is conducting local-to-state automated data sharing (but not workflow integration) with its Kaleidoscope and CJIN efforts. In addition, the TraCS effort managed by the DOT is a great example of a change in workflow to allow local law enforcement to communicate directly with local Courts. The significance of these efforts is that they allow for an entry

for disparate local systems to participate in a broader statewide information sharing effort.

With regard to local level readiness for integration, the survey the MAXIMUS/URL Team developed asked general questions, such as whether the extra work in implementing required business practice changes, more timely data entry, or changes in forms to support integration is worth it, despite the effort. In general, respondents agreed that the benefits derived from this effort would be worthwhile. Court administrators were the most optimistic that the effort to implement business practice changes would be worthwhile (83% thought the changes would be worth it), while the County Attorneys who responded were the least with 71% indicating that the extra work to support integration would be worth the effort.

Similarly, the survey asked whether it would be worth the effort to enter these orders and notifications into information systems and have these systems automatically notify interested parties such as law enforcement and community corrections, rather than making these notifications verbally, which is common practice currently in Iowa. Not surprisingly, local law enforcement and sheriff agencies reported seeing the most value in effort of conducting these notifications electronically, while Court practitioners and County Attorneys were more split on whether that would be a useful automated transaction. *This seems to be a common theme among the survey results: in concept, practitioners are supportive of CJIS, but are more interested in changing their business practice to facilitate automation if it makes their job easier, and less interested if it appears as if the business process change and/or automation would require more work.*

When asked to provide general comments on the usefulness of CJIS in Iowa, participants provided a wide range of opinions. Most that provided commentary agreed that the CJIS concept is necessary in Iowa; one respondent noted that "this is a great initiative. So much of the resources in this area are duplicated between agencies." However, for many respondents, the support was couched in concerns about how the effort would be implemented. There was significant concern about the costs of implementing CJIS, from a funding, staffing, and infrastructure perspective, as well as recognizing the current differences in business practices between large and small agencies in Iowa. One respondent noted:

> *"The main concern I have with standardization is that one size does not always fit all and the standardized forms are normally prepared to meet the needs of the larger jurisdictions and the smaller jurisdictions are then supposed to accommodate the changes. The other concern I have is that some of these changes will probably require the purchase of additional equipment, software, etc., and you have to be careful about the financial burden this may place on local agencies."*

Another respondent spoke to the importance of promoting an enterprise-wide view in support of CJIS:

> *"If information sharing is to work, the additional burden for data entry must be shared equally. If the burden falls primarily on one agency with that agency receiving little in benefits, then that agency will be resistant. This has happened in the past with Courts. Clerks of Court believe their data entry duties have been increased to help other agencies but they see little benefit in return to them or the judicial system as a whole for the extra work."*

In addition to these issues around business process change, standardization, and taking an enterprise-wide view of the responsibilities associated with CJIS implementation, there are other common themes that emerged from the survey responses and interviews:

- Most criminal justice practitioners are comfortable that information security can be maintained in an integrated environment;
- Practitioners are confident in their current policies, practices, rules, and statutes around information sharing;
- Participating in automation (e.g., sending information to the CJJP JDW, participation in TraCS) has required groups with disparate forms and business practice to come together and agree on a common approach;
- Current automated exchanges between agencies – whether state-to-state exchanges or local-to-state exchanges – are successful and improve the current business process; and
- The goals of automation and information sharing are to improve the business process and make important information readily available to justice practitioners despite the significant concern about the staffing burden that will be created if a CJIS solution is implemented.

3.3 Business Readiness Assessment

As highlighted in the previous studies, there were several business and planning/implementation themes germane to the business environment in Iowa:

- Focus on business process and forms standardization
- Developing a standards based approach – both for technical and business process issues – will be a significant change for most agencies
- Correlating array of identifiers currently in use by participating agencies
- Implement a phased approach and pilots where appropriate
- Resolution of public policy issues around information sharing and confidentiality

And as highlighted above, there are several themes associated with the As-Is Business Environment in Iowa, such as a general readiness to change current processes to participate in integration, confidence in the current rules and policies around information sharing, privacy, and security, and concern – especially at the local level – about the impacts of implementing a statewide integrated justice approach.

3.3.1 Enablers to CJIS in Iowa

The Enablers to CJIS in Iowa describes the successful initiatives, sharing agreements, and business processes that are providing a structure for the exchange of justice information sharing in Iowa.

3.3.1.1 Strong Governance and Planning Structures

The MOU between the Executive and Judicial Branches as well as the existence of the CJIS Board, the CJIS Advisory Committee, and a full-time CJIS Project Manager are important underpinnings to a strong governance and planning structure. This structure helps not only set direction for the CJIS initiative but helps coordinate existing efforts among the CJIS partners (e.g., County Attorneys pilot automation project, ICIS II development, and TraCS expansion) to ensure that all develop in a manner that suits their immediate business needs but retains the longer-term, enterprise-wide goal of information sharing.

The CJIS Advisory Committee has also demonstrated its willingness to provide resources in support of justice integration sharing. It has allocated grant funds from the U.S. Department of Justice, Office of Justice Programs (Edward Byrne Memorial State and Local Law Enforcement Assistance Act and National Governors' Association) funds to support the adult and juvenile exchange analysis as well as funding from the U.S. Department of Homeland Security to support the development of the Strategic Plan.

3.3.1.2 Successful Prior Automation Efforts

There have been several successful collaborations among agencies that speak to a readiness to expand and promote automated data exchange. Information is currently being shared between the DOC and the Judicial Branch around the PSI design and implementation. The project was funded through the CJIS office and was seen as a centrally coordinated integration effort. Although this project did not demonstrate a true transactional exchange between the agencies, it did meet the immediate business need. In addition, this pilot successfully addressed a business process flow issue around identifiers, in that the DOC carries the DCI# and FBI# that are key to positively identifying offenders. However, not all agencies have these identifiers in their system for all cases.

In addition, the success of the protection order transfer between the Judicial Branch and DPS is a very positive step and clearly demonstrates the capability of major state entities to exchange data in a workflow process. The transaction was not bound to the customary "stovepipe" data entry into DPS and allowed users not known or certified by DPS to directly enter into the IOWA System. This trusted host (server) that incorporates commonly agreed-upon security measures, is a necessary step in the integration effort. The transaction does not and should not compromise security and data integrity but it does offer a new paradigm for exchanges in Iowa.

In addition, the electronic disposition filing between these entities and the ability to match an agreed-upon tracking number (DCN) are examples of limited traceability that should be leveraged and replicated where possible.

In addition, there are several efforts that not only share state data but local data as well, such as Kaleidoscope and CJIN. Both of these systems consume and share local jail information, along with data from the state criminal justice systems. CJIN and Kaleidoscope have been very widely regarded by those agencies involved.

The upcoming County Attorney automation effort that will add 13 counties in automated case management software has tremendous promise in assisting that community in participating in a CJIS initiative in the future.

3.3.1.3 General Readiness to Integrate

There are several factors that position key State systems for broader statewide integration. For example, the current Court interface with DPS regarding protection orders and the CJIN effort that makes data available to Judges without going through the IOWA System provide practical examples of how DPS systems can exchange information, notwithstanding the stringent NCIC security guidelines and IOWA System Rules and Regulations. Creating exchanges that can be successful, while accommodating the differing security guidelines among these entities, suggests a readiness for and commitment to automated information sharing.

As mentioned above, local practitioners are generally ready to share information in an automated way and perceive the increased efficiencies associated with doing so, especially when it means making their jobs easier or making important information more readily available.

3.3.1.4 Strong Protocols Around Security and Privacy at All Levels

With the exception of Judges' concerns about whether data exchanged electronically is truly secure, practitioners at the State and local levels seemed uniformly comfortable with and confident in the policies that currently dictate the circumstances in which information from their systems is shared or passed to another person or organization, as well as with the information security protocols that help support that data transfer.

3.3.1.5 Strong State-Level Infrastructure

The strong systems at the State level also appear to be an enabler to a CJIS approach in Iowa for a variety of different reasons. The prevalence of the ICN, the common ICIS, TraCS, and the IOWA System network among law enforcement are well-established means by which communication occurs, especially between local and State agencies.

From the CJJP perspective, the JDW has the ability to play a larger role in gathering and analyzing data from these State systems of record. An integration effort would allow more readily available data to CJJP and bolster their ability to provide timely research

and statistics to key Iowa stakeholders. In addition, CJJP's organizational autonomy and reputation as an "honest broker" may assist in ensuring that systemwide interests are represented in the statewide CJIS implementation, rather than those of just one agency or branch of government.

3.3.2 Barriers to CJIS in Iowa

The Barriers to CJIS in Iowa discusses the current business practices and processes that must be overcome to achieve the objectives of the CJIS initiative in Iowa.

3.3.2.1 Limited Real-Time Data Exchange

The majority of current data sharing between agencies occurs via batch transfer, with the exception of the protection order interface between the Judicial Branch and DPS. Even for the batch transfer, there are limitations to how the data is used in many cases. For example, with information that is passed out of ICON, most of the receiving agencies do not attempt to bring the information into their systems for future processing; the information is placed in warehouses for queries based upon the DOC data representation and can, in some cases, be linked with other data primarily through named-based queries. The only exception to this is the transfer of offender data to the CJJP data warehouse, where CJJP attempts to match the data to other agencies data, primarily that of the Judicial Branch. The matching process is complicated and takes a significant number of cycles to process. The DOC indicated that they provided the method to match the data.

The Judicial Branch is dependent on the agencies filing cases with the courts, in that if they are not capable of automated exchange, there is currently not much the SCA can do. Currently, local law enforcement agencies and County Attorneys are not capable of electronic exchanges, with the exception of TraCS and other standard law enforcement exchanges operating via the IOWA System.

3.3.2.2 Disparate Security Requirements

The NCIC standards and IOWA System Rules and Regulations that govern DPS information systems make integration with those systems more challenging, since these standards are more stringent than those practiced by other justice agencies in Iowa. While there have been instances in which information is currently shared, real-time information sharing would require significant work to ensure compliance with these security requirements.

3.3.2.3 Need for Data Standards and Common Identifiers

Information in an integrated justice enterprise view needs to be available in three different ways: by individual, by incident, and by case. Currently, each system accounts for information based on the manner in which their component of the justice system uses it.

Law enforcement and Public Safety use the incident or DTN as the primary way of tracking an event. The DCI# is also used to tie together historical events to a positive person identifier. Law enforcement will of course use name, Date of Birth (DOB), etc., to query individuals as well, and often these are the only identifiers and there is no standard representation.

Conversely, the judicial process is case-based, and the Court case is the primary view. The Court case number is used to track the cases through the Court process. The Judicial Branch uses a person identifier, which links individuals across cases, but it is not tied to the DCI# or biometrically derived. Cases may be related, combined, or charges severed throughout the course of the process. This may result in further separation from the law enforcement incident representation.

The DOC is person-based using a DOC # to track the offender through the system. This number is retained and reused should the offender reenter the system. DOC must also track multiple sentences from multiple Courts to determine the offender's actual time to be held under the jurisdiction of the DOC. This is a complicated process as a sentence from one jurisdiction does not necessarily consider the sentence from another and the DOC is left to sort this out. Though the DOC retains the DCI# when received and the Court case numbers are on the sentencing documents, these are not used to track the offender or cases within the DOC.

Many of the numbers generated by the state agencies/branches are not provided back to local agencies for their use. Or if they are, they are often not incorporated into the local records management system.

3.3.2.4 Staffing and Infrastructure Concerns

Integration between systems for more than periodic batch transfers creates many benefits, but also places a level of responsibility upon the agencies that is quite different from what is now expected. The vision is a real-time exchange of information that is at least as current as the exchange of paper documents occurs, and that there is a basis of reliability among the systems to ensure it happens. Initially, this will require an adjustment in business practices, particularly real-time data entry into the agency's system; if the data is not in the system it cannot be transferred. If the paper precedes any electronic exchange and continues to be the primary exchange mechanism, the benefits of integration will not be readily apparent to the staff involved.

Supporting and maintaining systems is not new for the State agencies but will create challenges for local record management, jail management, and case management systems. Current staffing and infrastructure will not support the expectations of real-time transaction based exchanges.

3.3.2.5 Public Policy Issues Around Sharing of Information

Especially with regard to juvenile information sharing, there are several issues that arose during the Juvenile Exchange Analysis – the need for standardizing juvenile criminal history processes and juvenile Court documents, as examples – that need to be clarified by decision makers. These issues must be resolved before automation can occur in this area. Conversely, in the adult system, practitioners seemed very confident in and knowledgeable of the restrictions around information sharing with other agencies.

3.3.2.6 "Cultural" Issues Around Sharing of Information

Often the culture inhibits the sharing of information between justice agencies. This may take subtle forms in that the concept is embraced but when it comes to actually looking at pushing, pulling, and querying information from or to other systems, issues and concerns begin to emerge. These may take the form of concerns for security, data integrity, data ownership, or constraints placed upon an agency by external forces beyond their control, such as policy, code, and rules.

Iowa does have identified cultural differences or issues around information integration in a proposed transactional workflow environment, not unlike other states. However, Iowa, while not outright addressing these barriers, has instituted projects or exchanges that do in fact offer viable alternatives to the traditional "stovepipe" method for data entry and data query. These projects have set precedence, and this has opened the door to thoughtful approaches to breaking down the cultural barriers while maintaining the security and integrity requirements.

3.3.3 Summary

Iowa's current justice environment has made significant strides over the past several years in developing strong working relationships between the State agencies. This has resulted in a Memorandum of Understanding between the Judicial and Executive Branches. The MOU has set up a CJIS Advisory Board made up of both local and State representatives. The Advisory Board is guiding the arduous task of integrating Iowa's varied and disparate justice information systems.

The CJIS effort in Iowa is not just beginning with this project to develop a strategic plan, but has been evolving through a series of studies and projects geared toward gaining a better understanding of the complex business practices in Iowa, and in several cases implementing projects to address specific business needs. For many years the Executive Branch, through the Department of Public Safety, sought to automate the matching of arrest records and Court dispositions. To date, many states still use a manual process to update criminal histories. Iowa was successful in this project and maintains one of the higher automated disposition matching rates in the country. There have been many other gains mentioned in the body of this section for which both State and local officials should take pride.

However, as a part of the goals the justice community has set for itself over the last several years, coupled with the findings from the various studies that have been undertaken, the current environment highlights how much work is yet to be accomplished. The As-Is section of the plan set out to define a baseline from which the gaps between the goals and the current environment could be understood. Several key observations were made:

- The State has a very robust Justice Data Warehouse that is limited only by the lack of integration between the feeder agencies/branches.
- The State systems share information with each other, but this is primarily for the purpose of populating individual data warehouses to be used by the agency's/branch's stakeholders alone.
- There are diverse business practices in the justice community at the local level.
- Documents shared between agencies vary from jurisdiction to jurisdiction, but there is movement to standardize some of these forms.
- There are very few transaction-based exchanges. Where there are such exchanges they are successful but are currently held back by the technology employed. In addition, the successes have not been used as springboards to other similar, but perhaps more challenging, exchanges.
- The State agencies maintain unique representations of data that in some form all of the agencies do or could maintain. Examples of this would be name representation, demographics, and identifiers.
- The local agencies have disparate systems but do share common applications (TraCS) or are moving in that direction (County Attorney Case Management Systems).
- The justice leaders and practitioners, for the most part, have expressed a willingness to adjust their systems and practices to accommodate the CJIS initiative, which is seen as for the greater good.

The review of past studies, interviews with the State agency representatives, and the survey results all show the limitations of the current level of integration in Iowa. However, they do show how the strengths which are necessary to build a successful integrated justice information system and cognition of what it will take to move forward.

3.4 Technical Readiness Assessment

The purpose of the technical assessment of Iowa justice practitioners was to measure three important aspects of the current technical environment in the State. First, the assessment tried to measure how much technology is being utilized by the participating agencies. Second, the particular technologies employed by the justice community practitioners were assessed. Finally, the prevalence of new web-based technologies being proposed or used in information exchanges was sought.

In assessing the technical utilization of the participants, the assessment was trying to determine where each of the participants was in their current technology life cycle. The breadth and depth of the justice community is rather extensive. It is composed of multiple levels of government as well as multiple branches and each participant coming with its own business motivators and available funding sources. These diverse forces result in a wide array of technical profiles–even between agencies in the same jurisdictions that exchange information regularly. The gamut of environments can be described as having no technology support of the business process at all, to a fully integrated environment using the latest web-based standards and everything in between.

The ability to provide complete, accurate, and timely information to justice practitioners at key decision points in their business processes is heavily dependent upon having the appropriate technology in place. At a minimum, the technical environment must be composed of:

- Systems capable of capturing information needing to be exchanged in a manner that makes it available for others to use
- Networks that can carry the data to the appropriate recipients
- Security measures insuring the data is only available to authorized users

The measurement of these areas were the focus of the second objective in the As-Is Technical Assessment.

The third aspect asked participants to provide what steps Iowa justice practitioners had taken in adopting technologies that fit into the growing body of best practices being established for the justice community for automated information exchange. Among these technologies are eXtensible Markup Language (XML), web services, and service-oriented architectures (SOA). The rate of implementation and planned use of these technologies will provide a picture of what efforts already taking place in the State can be leveraged in the statewide implementation of the criminal justice information system CJIS Solution for the State of Iowa.

By measuring these three aspects of the environment, the MAXIMUS/URL Team will be able to create a baseline profile of the technology environment in Iowa. This baseline

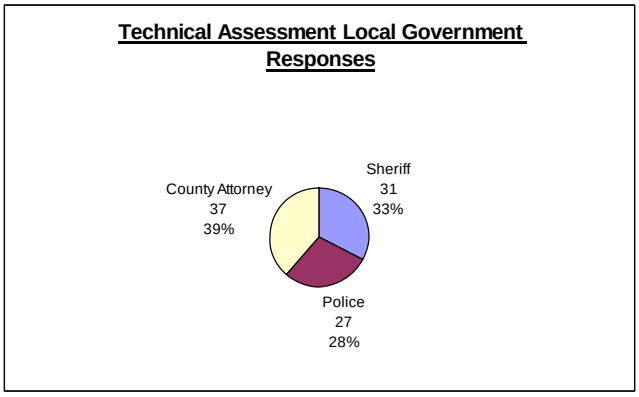
will allow the Team to determine what steps are necessary to implement the technical components that will facilitate information exchange in the eventual CJIS Solution. These steps will be an important element of the CJIS Integration Plan.

3.4.1 Description of Approach

3.4.1.1 Information Gathering

The baseline group of agencies identified to participate in the information gathering process included statewide executive and judicial offices as well as local city and county government entities. The CJIS Advisory Committee agreed to assist in the effort to solicit responses from the groups they represent on the panel. The following list is inclusive of the outreach made to gather data necessary to complete As-Is Technical Assessment work:

- Judicial Branch
  - State Court Administration
- Executive Branch
  - Department of Corrections
  - Attorney General's Office
  - Public Defender's Office
  - Department of Public Safety
  - Department of Transportation
  - Human Rights - Criminal and Juvenile Justice Planning
  - Department of Natural Resources
- Local City and County Government
  - County Attorneys
  - Sheriff Offices
  - Local Police Departments

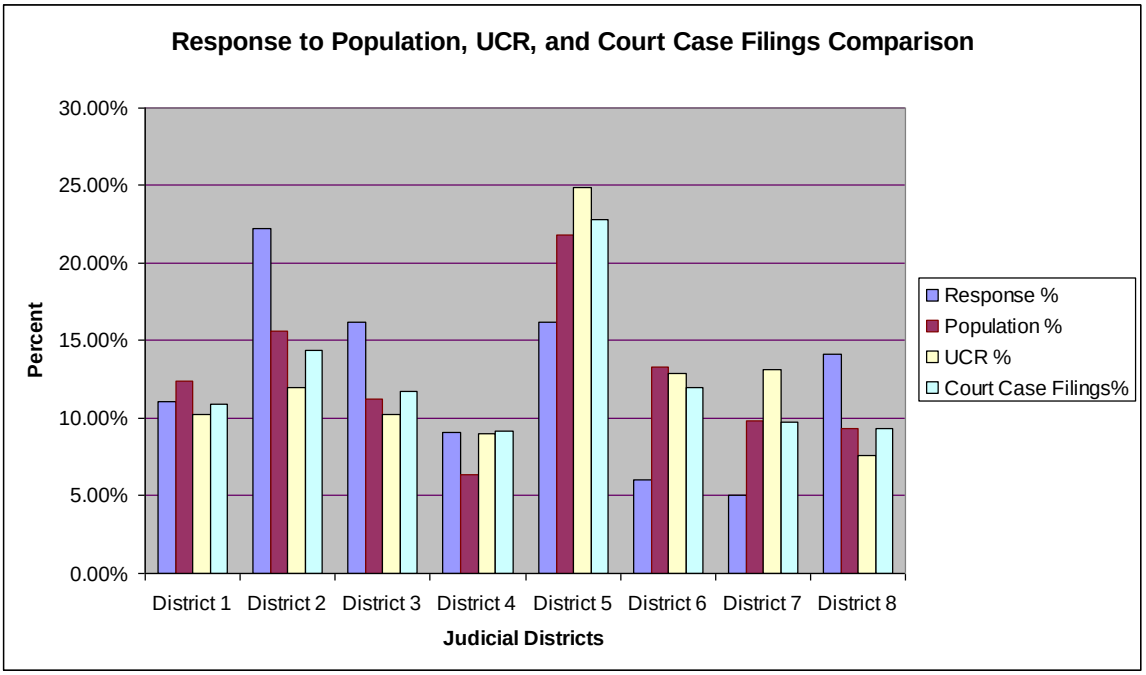


The unique role of the Judicial Branch as both a statewide and locally operating entity is a recognized reality by the MAXIMUS/URL Team. It is important to note that technical assessment did not solicit input from the local body of Judicial Branch members operating at the district court level because of the centralized nature of the Iowa Court's technical infrastructure administration. While the Iowa Court Information System (ICIS) application is distributed across the State, its components are managed from the State Court Administration Office in Des Moines. The locally-based judiciary representatives were part of the group information was gathered from for the As-Is Business Readiness Assessment.

The MAXIMUS/URL Team employed a variety of approaches to collect the information represented in the As-Is Technical Assessment. These approaches included:

- Researching previous studies and ongoing technology acquisition projects related to the Iowa justice practitioner's technical environment
- Interviewing system administrators and technical resources currently supporting the technical infrastructure in Iowa
- Surveying system administrators, technical resources, and other knowledgeable resources about the state of technology in their respective agencies

In total, the Technical Assessment gathered information from over 100 Iowa justice practitioners spread across 69 counties. The local level respondents to the technical survey were located in all eight of the Iowa Judicial Districts. The following graph demonstrates the percentage of responses received compared to the percentage of Iowa's population residing in the judicial district,[20] the percentage of crime reported by the Iowa Uniform Crime Reporting (UCR) program,[21] and the percentage of court case filings in each judicial district.[22]



[20] Population as projected by the State Data Center of Iowa for 2003 (http://www.silo.lib.ia.us/specialized-services/datacenter/index.html).
[21] Incident-Based Iowa Uniform Crime Report 2003 Release Part II Statistical Data Table 1
[22] http://www.state.ia.us/dhr/cjjp/images/pdf/CaseFilings2003.pdf.

3.4.1.2 As-Is Technical Assessment Section Descriptions

The MAXIMUS/URL Team has adopted a framework to describe the numerous technical infrastructures that occur among Iowa's justice practitioners. The framework provides a consistent means to understand the important aspects being measured in the As-Is Technical Assessment portion of this document. The information gathered for each of the survey groups will be aggregated into the following high-level areas by domain:

- **Current System Environment:** The Current System Environment section will provide a detailed look at the hardware, operating systems, relational database management systems, application servers, etc., in Iowa that are expected to be leveraged in the automated exchange of justice information. This information will be presented with additional sub-sections pertinent to the particular system category and survey group.

- **Current Network Environment:** The Current Network Environment section will provide a detailed view of the network connectivity (Internet, IOWA System, ICN) in the State and local agencies that are expected to participate in the CJIS initiative.

- **Current Security Policy:** The Security Policy section review will assess the current security models encryption, etc., being utilized by the survey participants to protect their networks and applications.

- **Data Standards:** The Data Standards section will examine how data being shared in Iowa is formatted and the metadata standards such as XML and NIST EFTS currently being used in the Iowa justice community.

- **Transaction Processing Capability:** The ability to create and process transactions in an event-driven environment using a guaranteed messaging framework (MQ, java messaging service, WS-Reliability) will be measured in the Transaction Processing Capability section.

- **Adoption of Web Service/SOA Standards:** A mandatory requirement of the RFP is that the recommended CJIS solution be based upon web-based standards. This section of the document will depict what the current adoption of these types of standards is in the Iowa justice community.

3.4.2 Judicial Branch

When ICIS began, it was implemented locally in each Iowa judicial district and county. Since then, due to shrinking resources and shortcomings identified during the regular three-year internal reviews/gap analyses, ICIS was consolidated from local implementations in each court to regional implementations housed both at the Justice Building (JB) and Joint Forces Headquarters (JFHQ). This is the still the current architecture, which is made up of 26 database/forms application servers hosting the

system statewide. Thirteen of the database and application servers are housed in the primary data center at the Justice Building, and the other 13 servers are housed in the alternate data center at JFHQ.

The current ICIS system is an Oracle Forms application using an Oracle Relational Database Management System (RDBMS). The application and database layers are hosted on IBM RX/6000 servers running AIX. Oracle Forms 6 is the application server software, and Oracle RDBMS 8i is the version of the database platform. Application software, in addition to the ICIS functions, includes Microsoft Word, which supports word processing, and Lotus Notes electronic mail as well as other office-oriented tasks. Public access to Judicial Branch information is housed on separate application servers in the Hoover building using IBM WebSphere as the application server software. A given county will use this entry into the ICIS system to retrieve information about another jurisdiction. ICIS is currently in the process of migrating the ICIS front-end software to a web-based Java application using Oracle 10g iAS Application software hosted on Dell Linux-based application servers with centralized database and application server clusters to support all courts by December 2005.

3.4.2.1 Network Connectivity

The ICIS system is accessed statewide via the fiber of the Iowa Communications Network (ICN) WAN. The ICN has a point-of-presence in each county and from it, local telecommunications companies provide connectivity to the ICN WAN for each locale. A T1 line is accessible for each county and while appropriate for larger court offices, it is somewhat less useful to the smaller jurisdictions. The SCA has approached both DPS and the DOC as to the feasibility of sharing these underutilized connections; but at this point, no commitments have been made by DPS or DOC regarding the use of these established local feeds.

The SCA utilizes the ICN exclusively to support statewide connectivity for the ICIS system. The only exception to this is a direct connection from the Justice building data center to the 8th Judicial District. The SCA has an agreement with the ICN that allows it to manage the agreements with local telecommunications companies in providing the necessary local connectivity to the ICN inclusive of consolidating the monthly billing. The SCA has established service level agreements with the ICN to ensure that measurable and sufficient uptime and reliability is provided for the ICIS users. However, this sometimes involves significant follow-up by the SCA in order to keep the level of service in line with the current agreements. Taken together, this allows for ICIS to utilize statewide connectivity at a local level without having the burden of the hands-on administration of ICIS network connectivity.

3.4.2.2 Current Security Policies

The ICIS application is a secure application utilizing a Lightweight Directory Access Protocol (LDAP) maintained by the SCA office. At the lowest level of entry, all ICIS users are authenticated by username and password. Network access for users is

controlled by firewall and access control list configuration on the ICN. This configuration is done by the ICN staff at the direction of the Judicial Branch. Since ICIS handles financial transactions in daily business processes, the system–and especially the system security policies–are audited by the State Auditor's office as well as reviewed internally by the SCA office during its gap analyses studies. At this time, all of these reviews and analyses have concluded that there is no need for any changes to the ICIS system security policies.

3.4.2.3 Data Standards

As the current interfaces with ICIS are single processes to fit a specific need for sharing information, data standards for such interfaces, while well-defined, are limited to meeting the needs of the individual interface. FTP transfers of flat files are the most prevalent method of data exchange, and the structure of such files necessarily follows a format specific to the needs of the processes and systems that ICIS is exchanging data with. Broader data standards such as the utilization of XML, XML schemas, or GJXDM to provide a common structure for data exchanges are not currently implemented and as such, not utilized in any of the interface processes with ICIS. This is not to suggest, however, that ICIS as a system is incapable of working with standardized data formats such as XML; on the contrary, the SCA fully embraces the value of such common data standards for exchanges and is technically capable of providing data in any current and future exchanges in this manner. Recently, the State Court Administrator's office worked jointly with the Department of Transportation to arrive at a common set of XML-based data exchanges. While that effort has not yet produced a final set of standards, such work to move towards the use of common data standards is ongoing.

3.4.2.4 Transaction Processing Capability

Currently, interfaces with the ICIS system are done mostly by flat file FTP transfers that are conducted on scheduled intervals. An exception to this is the protection orders interface with DPS. In this interface, ICIS users enter protection orders into their system, which are then sent real-time to DPS via the switch. To affect this exchange, the structure of these orders is modified to appear as a switch transaction. This represents a shift from the batch process type of interface to one where users from the ICIS system exchange data with DPS as a part of their daily business, with the entry of Protective Orders being the trigger to send data to DPS. From a technical standpoint, these established interfaces with DPS and other statewide CJIS partners present established inroads towards evolving such interfaces into event-driven transactions within a workflow.

3.4.2.5 Adoption of Web Service/SOA Standards

While not currently making use of a transaction-based workflow to manage interfaces with ICIS, the current system is well positioned to do so. In utilizing Oracle 10g iAS as the application server software, industry standards of service-oriented architecture are already available to ICIS. It is not anticipated that the current ICIS architecture presents

any technical hurdles to implementing a service-oriented architecture with respect to integration.

3.4.2.6 Technical Readiness Summary

Overall, the ICIS system offers the Judicial Branch a system capable of being enhanced to participate in an integrated justice environment. This is particularly evident by the upgrade of the ICIS system from an Oracle Forms application to a web-based Java application at the end of this year.

Several inroads to integration have already been made with existing interfaces identifying areas of data exchange. And with the example of the protection orders interface with DPS, interfaces with ICIS are already moving towards a transaction-based design. While no service-oriented architecture is currently in place, the use of XML is burgeoning as recognized by efforts with the Department of Transportation to standardize the format for citation data.

The SCA has made a commitment towards moving forward with a statewide integration effort. Technically, they are well positioned to enhance the ICIS system to transform existing interfaces to implement a service-oriented architecture approach. However, analysis and development work will need to be done to move existing batch interfaces to transaction-based exchanges as well as redefine the structure of the data into XML-based formats.

3.4.3 Department of Corrections

3.4.3.1 Current Systems Environment

The Iowa Corrections Online Network (ICON) was developed for the DOC and is maintained in cooperation with Advanced Technologies Group, Inc. (ATG), a software vendor-based in West Des Moines, Iowa. The system is hosted on-site at ATG offices.

The current ICON system as provided by ATG is a complete Microsoft solution. HP Proliant servers make up the hardware platform for both the application and database layers. Web and database servers all run MS Windows 2000 utilizing MS SQL Server 2000 for the database layer and Microsoft IIS 5 for the application layer. Both the application and database layers have their servers in clustered environments for failover and load balancing. The primary data center site is hosted at ATG with an alternate hot-site hosted at the Department of Corrections for disaster recovery failover. Near real-time backups are propagated approximately every 90 seconds from the primary ATG data center to the hot site at DOC. In case of ATG site failure, ICON users are redirected to the DOC hot site through network routing, without the need to make individual user changes or application/database server changes.

3.4.3.2 Network Connectivity

ICON is accessed statewide via the ICN WAN. The DOC uses the ICN exclusively except for some users within ATG and DOC who have direct connections to the ATG data center. The administration of ICON network connectivity has been and continues to be a joint effort between ATG (on behalf of the Department of Corrections) and the State ICN staff. ATG was responsible for the initial router and switch configuration and works closely with the ICN staff to ensure that the specific configurations are maintained. The DOC, with the assistance of ATG, is very satisfied with the use of the ICN to support its statewide user base and sees it as a viable network infrastructure to support statewide integration.

3.4.3.3 Current Security Policies

ICON users are authenticated to the system via username and password. The Department of Corrections maintains user authentication credentials and ICON levels of access via a separate security maintenance application provided to them by ATG. All ICON users must first be identified, approved, and set up via this security application before they can use the ICON system. All access, inclusive of properly authenticated access, is captured as history for review and audit as necessary. Additionally, network access to the ICON system is controlled through the ICN by firewall configurations and access control lists maintained by ATG at the direction of the DOC.

3.4.3.4 Data Standards

The ICON system, as provided and administered by ATG, is currently well positioned to make use of data standards such as XML, XML schemas, and GJXDM. ATG has a strong commitment to common, structured data standards and is already experienced in XML-based interfaces. Consequently, in that context, the ICON system can be considered XML "ready". However, as with many of the existing interfaces throughout the Iowa CJIS community, custom flat file transfers are the prevalent form of data exchanges with ICON. These interfaces meet the needs of specific exchanges with specific partners and do not necessarily demonstrate the consistent use of a common structured data format that could be considered standardized. The ICON interface with the ICIS system for Pre-Sentencing Investigation (PSI) orders, while batch in nature, does not utilize flat file data transfers but a separate staging database maintained by the State Court Administrator's office. The ICIS and ICON systems utilize SQL statements for data entry specific to this staging data structure.

3.4.3.5 Transaction Processing Capability

Data exchanges that occur as real-time triggered events within an accepted workflow process across the Iowa CJIS community are not part of the current interfaces with ICON. Aside from PSI orders, current data exchanges are flat file transfers via FTP that are scheduled rather than event-driven, real-time aspects of a process-driven workflow.

From a technical perspective, ATG is capable of supporting the DOC in augmenting the current ICON system to be a transaction-based on its data exchanges with both the Judicial Branch and the DPS.

3.4.3.6 Adoption of Web Service/SOA Standards

Even though a transaction-based workflow is not currently used to manage data exchanges with DOC, the current ICON system is implemented on Microsoft application server technologies, and as such, the Department of Corrections, through ATG, can more than adequately leverage industry standard practices of service-oriented architectures. Consequently, the current ICON system, while currently not SOA-based for data exchanges, has no inherent impediments to adopting a service-oriented workflow.

3.4.3.7 Technical Assessment

With ICON, the DOC has a mature system capable of being enhanced with exposed web services and the use of XML in a transaction-based workflow for data exchanges. While DOC would rely heavily on ATG to transform the design of existing ICON interfaces, ATG possesses the necessary skill sets required to do the work.

Currently, data standards are still structured flat files specific to the individual interface needs. Real-time triggered events are not part of the existing exchanges as they are still batch in nature. An exception to this is the use of Kaleidoscope to retrieve more up-to-date probation and parole information. Design and development work would be needed to transform the existing ICON interfaces to a service-oriented architecture, exchanging data as the result of triggered events within an established workflow.

3.4.4 Attorney General

The Iowa Attorney General's Office is heavily involved in several aspects of the Iowa criminal and juvenile justice processes. Forefront among these is the prosecution of serious felonies and the preservation of convictions and sentences won by the County Attorneys. Information concerning the current technical environment of the Attorney General's Office was obtained using a survey tool available via the Internet. The information is fairly abbreviated, but provides a good baseline of where the agency is in its current technology life cycle. Maintenance of the environment is provided by a small staff of one or two resources.

3.4.4.1 Current Systems Environment

The Attorney General's Office uses a vendor supplied COTS tool for their Case Management System (CMS). The ProLaw application (v 7.86i) from Thomson Elite, is one of the two applications selected in the Iowa County Attorney Case Management

System Project currently being tested and implemented in 12 local agencies. Other areas of investment in the current system environment include:

- The deployment of a .NET platform independent tool
- Use of the IIS application server
- Use of SQL Server as the database server

3.4.4.2 Network Connectivity

The Attorney General's Office maintains connectivity to several major communications networks. The ones specifically identified by the Department were the ICN, the IOWA System, and the Internet. All of the connections to these communication infrastructures were at broadband speeds.

3.4.4.3 Current Security Policies

The Attorney General's Office relies mainly on firewalls for the protection of its systems and network from unauthorized access or use. The survey response did not indicate that the agency is utilizing any encryption or authentication in its current security policy.

3.4.4.4 Data Standards

The Attorney General's Office also indicated that it did not currently import or export data from its systems for use by other automated applications. The definition of flat file structures, NIST EFTS transactions, or XML documents is not currently employed in the Office for either sending or receiving information from partner agencies.

3.4.4.5 Transaction Processing Capability

The Attorney General's Office did not respond to the questions regarding their use of guaranteed messaging architectures such as MQ Series, JMS, or WS-reliability. This response is consistent with the indication that the agency was currently not sharing information with other partner agencies. There was also no indication that they were using a non-network medium such as tapes, CD or DVD, or floppy disk, to share data with other agencies.

3.4.4.6 Adoption of Web Service/SOA Standards

There was no indication of the adoption by the Attorney General's Office of a web service or SOA standards in the survey.

3.4.5 Public Defender

The State Public Defender oversees and coordinates representation to indigent persons in legal matters such a being charged with a crime, in juvenile cases, and on appeal in criminal and post-conviction relief cases. This representation may be provided through either the State Public Defender Office attorneys or through private attorneys who contract with the State Public Defender. Private attorneys may also be appointed by the Court to in lieu of a formal contract. The Public Defenders Office is headquartered in Des Moines and has 19 field operations throughout the State. Information for the As-Is

Technical Assessment of the Public Defender Office was gathered using an online survey. The office maintains a small staff of one to two people for its IT support purposes.

3.4.5.1 Current Systems Environment

The Public Defenders office is currently utilizing a custom-built application for the handling of their case management. The user interface, database, and application platforms were not disclosed in the response for the solution. The office has not begun the implementation of platform independent tools such as Java or .NET at this time.

3.4.5.2 Network Connectivity

The Public Defenders office maintains a broadband connection the State ICN but does not have connection to the IOWA System or the Internet.

3.4.5.3 Current Security Policies

To protect their data and their networks from unauthorized access, the Public Defenders employ multiple security policies. These include the use of authentication, encryption, and firewalls in their IT infrastructure.

3.4.5.4 Data Standards

The Public Defenders do not currently import data to their own system or export information out for support of a partner agency's business process. They are not utilizing any formal data structure in their current operation such as flat file, NIST EFTS, or XML.

3.4.5.5 Transaction Processing Capability

As the Public Defenders do not currently share information electronically, there is no use of a guaranteed messaging protocol such as MQ Series, JMS, or WS-Reliability. There is also no utilization of a non-network medium such as tape, CD, or floppy disk.

3.4.5.6 Adoption of Web Service/SOA Standards

The Public Defenders are not currently employing or have near-term plans to use web services or SOA standards in its technology platforms.

3.4.6 Department of Public Safety

3.4.6.1 Current Systems Environment

3.4.6.1.1 Kaleidoscope

Built by software vendor Datamaxx Enterprise Intelligence, Inc., Kaleidoscope effectively integrates critical State and local data, allowing it to be accessed over the communications infrastructure of the DPS statewide network. This accessibility provides valuable and timely information sharing regarding offenders who have been released into community-based supervision programs managed by the Department of Corrections and those detained and/or released pending trial from the Polk County Sheriff's Detention

facility. During routine traffic stops, law enforcement officers are notified of an individual's status as a probationer or person awaiting trial.

3.4.6.1.2 IOWA System

The IOWA system is currently implemented on an IBM RS6000 AIX two-node cluster running Oracle 8i Enterprise Edition. Additionally, this cluster is used to support the Open FOX message switch.

The use of the IOWA System is substantial and it represents a significant portion of the justice related data in the State of Iowa. It is utilized by all State and local law enforcement agencies as well as the main conduit for connections to the National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (NLETS). DPS maintains several interfaces with the IOWA system along with the daily use by law enforcement agencies amounting to tens of millions of messages processed a year. The primary access to the IOWA system files is through the Open FOX message switch that validates user credentials by location (ORI) and terminal identification.

3.4.6.1.3 Automated Fingerprint Identification System

The Iowa Automated Fingerprint Identification System (AFIS) is an electronic repository of fingerprint data. When used in conjunction with Livescan machines in select municipal, county, and corrections facilities, the process of positively identifying an individual and capturing arrest data associated with the fingerprint card is a near real-time event. In addition to the receipt of the arrest data in the criminal history repository, an assigned a Division of Criminal Investigation (DCI) number is returned to the arresting agency as part of the Livescan transaction.

3.4.6.2 Network Connectivity

Since access to DPS systems is used by law enforcement agencies statewide, the ICN WAN is used as the network infrastructure. The ICN has a point of presence in each county, and like the State Court Administrator's office and the Department of Corrections, local telecommunications companies provide the "last mile" link between the local law enforcement agencies and the ICN. The ICN helps coordinate billing for these connections for DPS, specifically the Division of Administrative Services, Technology Services Bureau (TSB). TSB monitors its use of the ICN network and administers it through the use of service level agreements with the ICN staff whereby specific access policies and protocols mandated by TSB and NCIC are enforced. From the DPS data center, there are three DS3 lines to the ICN point of presence in Polk County with routers on each end maintained directly by TSB. Remote users connect up to the ICN with point-to-point 56 Kbps circuits. Such direct connections are required for the enforcement of security policies mandated by NCIC and IOWA System Rules and Regulations. DPS, by Iowa statute, cannot be recognized as an Internet service provider.

3.4.6.3 Current Security Policies

IOWA system users are required to first be trained and NCIC certified before access is granted. Username and password authentication is in place at the lowest level of security; however, each user is also identified by location as well as the identification of the terminal used. Firewall configuration, access control lists, and direct point-to-point connections for IOWA system users are enforced by the TSB. Additionally, almost all of the IOWA system transactions (both query and update) against the CCH and hot files are routed through the message switch.

3.4.6.4 Data Standards

Some of the DPS interfaces with ICIS and the Department of Transportation utilize flat file transfers processed in batch, but there are significant inroads that have been made towards the use of XML. These interfaces exchange XML documents via web services that are built using the Open FOX markup language (OFML) standard that is recognizable to the message switch. Additionally, internal rap sheet generation is GJXDM-compliant, however, will not be passed along to the IOWA system user community until later this year. The same GJXDM compliance will apply to DOT interfaces especially after the Driver's License system is upgraded in early 2006, further allowing the exchange of images.

3.4.6.5 Transaction Processing Capability

There are three examples of existing interfaces with the Department of Transportation that utilize a transaction-based data exchange. The first is with the legacy DOT Driver's License system. This is a mainframe-based system, and DOT has allowed DPS to build and maintain transactions that are utilized to retrieve driver's license information. DPS is able to make requests via this transaction to this mainframe system in real-time to satisfy driver's license inquiry processes. The second and third are existing interfaces with the DOT Vehicle Registration and Reciprocity systems (none merged). These are both web-based applications and affect an interface with DPS by exposing a web service that DPS access as a client to the web service. As mentioned above, the data is exchanged is formatted as XML with a markup standard specific to the IOWA System message switch.

Additionally, the interface with ICIS for protective order entry is somewhat transaction-based as the event of entry in ICIS triggers the order to be sent over to the IOWA system. This effectively makes the ICIS users IOWA System users although this is mitigated by the layer of abstraction provided by the ICIS system itself as well as the protective order data being structured as a message switch transaction with accompanying ORI information, confirming terminal identification, and user contact telephone and fax numbers.

The use of Livescan devices to capture fingerprint and arrest data electronically is further example of transaction-based processing with the IOWA system. In a near real-time process, Livescan transactions utilize AFIS to make identifications, update the AFIS repository, and update the IOWA system with arrest information. The final part of this

transaction sends not only identification results back to the arresting agency but the assigned DCI number as well.

3.4.6.6 Adoption of Web Service/SOA Standards

Technically, DPS–and specifically the IOWA system–can approach a service-oriented architecture in somewhat limited fashion. The switch is scheduled to incorporate web services in its design in September 2005. Since the message switch is the primary conduit for access to the IOWA system, service-oriented access to DPS can become far more readily available than it is now. DPS already has in place the utilization of data exchanges real-time with the above-mentioned systems that expose web services for the exchange of Vehicle Registration and Reciprocity data.

3.4.6.7 Technical Assessment

The Department of Public Safety appears to be in a state of transition between traditional methods of interfacing with other agencies and more current transaction-based data exchanges. Access to the IOWA system via the message switch represents tried and tested methods for data retrieval and updates that comport with existing methods established within the NCIC model. However batch flat file interfaces, real-time Protective Order data entry, AFIS and Livescan transactions, and transaction-based XML data exchanges with DOT represent inroads to updating access to the IOWA system to a truer integrated environment. This is especially true when considering the DPS commitment and readiness in the use of GJXDM and the design update of the Open FOX message switch to make service-oriented architecture a reality.

It should be noted that one of the primary missions of the DPS is to ensure not only the integrity and accuracy of the data that resides in their systems but the security of it as well. Any move forward by DPS towards a transaction-driven, service-oriented architecture must enhance the efficiency of their mission and the overall value of the services they provide but still preserve their primary charge of ensuring a secured environment for the data they are responsible for.

3.4.7 Department of Transportation

3.4.7.1 Current Systems Environment

3.4.7.1.1 TraCS

In 1994, the Iowa Department of Transportation (DOT) partnered with other State and local agencies to develop a statewide accident reporting system, promoting efficient and accurate capture of accident related data. The Mobile Accident Reporting System (MARS) was an initial component of the Officer Information Manager (OIM). In 1997, the State of Iowa was selected by the Federal Highway Administration (FHWA) as a partner in the National Model Project to expand and promote safety data collection. In

2000, the OIM system became known as the Traffic and Criminal Software system (TraCS), and in addition to MARS, includes the following components:

- Electronic Citations Component – ECCO
- Mobile Implied Consent for Operating While Intoxicated – OWI
- Commercial Motor Vehicle Safety Inspection – VSIS
- Incident-based reporting – CIRF (NIBRS compliant)
- Geographical Information System (GIS) Location Tool

TraCS represents the field data collection technology of the National Model in the State of Iowa and the primary system in use for law enforcement with respect to motor vehicle violations. It is also emerging as a system for capturing criminal complaint data collection. A significant part of the TraCS effort has involved working to standardize forms used to capture citation and accident data across the State and to enhance the TraCS system to accurately and efficiently capture such data through a notes-entry interface.

The system is implemented as two distinct parts. Mobile units utilize TraCS Mobile with either a notebook or pen-based computer. With TraCS Mobile, officers can capture and validate all entry necessary at the scene inclusive of diagrams, image attachments, GIS location information, and electronic signatures. Data gathered locally via TraCS Mobile is then downloaded to TraCS Office. TraCS Office is an agency-level implementation of the TraCS system, and in addition to the functionality of TraCS Mobile, includes a repository database hosted by Microsoft Access 2000, Microsoft SQLServer 2000, or Oracle 9i. From the TraCS Office system, citation data is uploaded to file servers at DPS. The citations are picked up by the ICIS system for adjudication. This data is then transferred via FTP back to the Driver's License system at DOT.

3.4.7.1.2 Motor Vehicle and Driver's License Systems

Currently, the Motor Vehicle and Driver's License systems are on two different technology platforms. The Driver's License system is currently a legacy COBOL application hosted on the State MVS mainframe system using VSAM file structures. Vehicle Registration is a more current web-based application running a Windows 2003 server operating system, Microsoft IIS6 web server, and a SQL Server 2000 database. The Driver's License system is slated for upgrade to the same architecture as the Vehicle Registration system in March 2006.

3.4.7.2 Network Connectivity

TraCS makes use of wireless and local network connections to implement the transfer of data between TraCS Mobile and TraCS Office. However it is the TraCS Office data exchanges between DPS, the Judicial Branch, and DOT that are germane for the discussions of statewide integration readiness. As is the case with DPS, DOC, the Judicial Branch, and the JDW, TraCS and the Motor Vehicle/Driver's License systems utilize the Iowa Communication Network (ICN) statewide fiber network for connectivity

to the participating systems. Additionally, information regarding driver's licenses, vehicle registration, and reciprocity are currently exchanged with DPS via the State message switch. The established use of the ICN as well as the established use of communications with the Iowa On-line Wants and Warrants system provides DOT with a technical network readiness to participate in an integrated data exchange environment.

3.4.7.3 Current Security Policies

The Driver's License, Vehicle Registration, and TraCS systems all rely on username/password authentication at their fundamental level of security. This applies to system user authentication and FTP authentication for flat file transfers. Currently, LDAP is not employed to manage user accounts or authentication. While TraCS utilizes a DPS file server as the central location for distributing its various reports to the courts, it is not considered in the same context as an NCIC/NLETS terminal connection, and consequently, no location, terminal, or user information is included with the files. In addition, TraCS is currently not using encryption for its data transmissions, and when files are moved the DPS file server, these are considered to be utilizing the already secured and trusted network environment of the ICN for purposes of communicating with DPS. Also, interfaces with respect to Vehicle Registration and Driver's License that update master indexes used in off-line searches are delivered to DPS in cartridge tape or DVD and uploaded manually. These represent a significantly off-line and trusted policy with respect to exchanging data.

3.4.7.4 Data Standards

The Department of Transportation systems, especially TraCS, are currently the most closely aligned with the use of standard data formats and specifically XML. Since TraCS must interface with many local, state, and federal systems, it necessarily has the capacity to present accident, citation, and complaint data in various formats. TraCS has a "transmission builder" component that renders the data in a custom XML format, given a .btx extension. This document is then further modified via an XSLT transformation to produce a structure or file format compatible with the local, state, or federal entity involved in the exchange. Currently, TraCS provides data on citations, accident reports, safety inspection, and roadside damage as shared or integrated data sets.

The Vehicle Registration and Reciprocity systems already utilize an XML-based data standard for their current data exchanges with the Department of Public Safety. The data in these exchanges is not currently GJXDM-compliant; however, both DOT and DPS are already positioned to enhance these data exchanges to be so.

Overall, DOT is closer to utilizing common data standards as the use of XML is already incorporated in the data exchanges for the TraCS, Vehicle Registration, and Reciprocity systems. With respect to the major State systems, the formats of DOT data exchanges still represent custom, entity-specific structures for these data exchanges even through the use of XML.

3.4.7.5 Transaction Processing Capability

The development of TraCS into an efficient safety data collection system has necessitated analysis of the existing workflow of reporting accident data and implementing the steps to make that workflow more efficient. However, interfaces with TraCS have not implemented those identified workflow steps into a transaction-based set of data exchanges. Yet the DOT Driver's License, Vehicle Registration, and Reciprocity systems are very much transaction-based in their current data exchanges with DPS. The Driver's License system is mainframe-based, and DPS maintains a CICS transaction on that system to support real-time requests of driver's license data. Vehicle Registration and Reciprocity have real-time data exchanges with DPS via their current web-based service architectures.

3.4.7.6 Adoption of Web Service/SOA Standards

Although the continuing enhancement of the TraCS system is moving towards the adoption of a centralized service-oriented architecture, TraCS does not currently utilize such architecture for data exchanges. However, the DOT Vehicle Registration and Reciprocity systems currently exchange data with DPS via web services. The Driver's License system does not currently use a service-oriented architecture; however, this is proposed for early 2006 when that system is moved from the mainframe environment to a Microsoft-based web application running Microsoft IIS6 and SQL Server 2000.

3.4.7.7 Summary

With respect to common data standards in the use of XML, transaction-based processing, and the existing use of service-oriented architectures, the Department of Transportation systems already employ the features of an integrated data exchange design to some degree.

The TraCS system currently streamlines the workflow of collecting and exchanging traffic and accident data as part of its charter and is making inroads to moving its interfaces exposed via a service-oriented architecture. The Driver's License, Vehicle Registration, and Reciprocity systems already are transaction-based in their data exchanges with DPS, while the Vehicle Registration and Reciprocity systems already utilize web-based services and structured XML data in their exchanges.

The Department of Transportation has several systems that are already at or are moving quickly towards a true integrated data exchange environment, have a need to ensure that their efforts are coordinated and ultimately bring all systems up to a common level of efficacy with respect to XML usage, transaction-based processing within a workflow, and the use of web-based, service-oriented architectures.

3.4.8 Division of Criminal and Juvenile Justice Planning

3.4.8.1 Current Systems Environment

The Justice Data Warehouse (JDW) is a component of a larger statewide Enterprise Data Warehouse system. The JDW is managed by the Iowa Division of Criminal and Juvenile Justice Planning (CJJP), and is a data warehouse housed on a NCR4800 two-node cluster. Teradata is the software provider for the data warehouse and accompanying load and query tools such as Teradata Multiload and Teradata Fastload. A Microsoft NT server acts as the staging server where all data from DOC's ICON system and the Judicial Branch's ICIS system is staged before being loaded into the warehouse. JDW users access the warehouse for reports using the Microsoft IIS Web-i application server housed at the Hoover building.

3.4.8.2 Network Connectivity

The JDW user community is statewide and utilizes the ICN WAN for connectivity to the JDW for remote sites and the State Capitol LAN for users in Des Moines.

3.4.8.3 Current Security Policies

Access to the JDW is limited to the use of Business Objects for running reports that are further broken down by access, based on the type of data. Judicial data from ICIS is separated by either adult or juvenile and corrections data by prison or community-based corrections (CBC). Typically, Judicial Branch users see only data populated by ICIS, and DOC users see only data populated by ICON; however, there are some research users that are authorized to see both. User account information is maintained by CJJP within the Business Objects application, and users are authenticated by username and password validation at the application layer.

3.4.8.4 Data Standards

All data exchanges with the JDW are done as monthly batches to the JDW staging server. The structure of these flat files are specific to both the systems of origin and the structure of the data models that are loaded. Additionally, these files are not currently structured to present data from a transaction, trigger-based event in real-time, but rather as a collection of data from a month's time. While far removed from a real-time integration design, this works well for the repository nature of the JDW, especially when considering the extract, transform, and load (ETL) work required. Additionally, the repository nature of the design necessitates the collection of data that is retrieved by reports and data mining research efforts. As such, data standards for building these reports are tailored for each report, although the content for these reports could be structured as XML to make their content more portable. CJJP would need to explore the feasibility of using of XML with Teradata to ensure that the existing warehouse architecture could support it.

3.4.8.5 Transaction Processing Capability

Currently, no transaction processing features exist for data exchanges with the JDW. This is not necessarily because of a technological oversight, but rather due to the nature of the JDW design. As a warehouse, the JDW is built to receive data, store it, and structure it to support research and analysis efforts. Reporting on the data is done within the context of these research efforts and as such, is confined to their specific directions and schedules. Traditionally, real-time transaction processing is not usually part of a warehouse environment. There are not any technical roadblocks preventing the transfer of data from the Judicial Branch or the Department of Corrections in a transaction-based manner as part of a workflow. However, there would be some effort required to rework the ETL process, and time required to complete such processing could impact the real-time nature of the transactions.

3.4.8.6 Adoption of Web Service/SOA Standards

The data loads into the JDW and the subsequent reporting on that data are not currently implemented in a service-oriented architecture. Reporting could be more easily structured as a service given the current implementation of Business Objects as a web-based application. However, data loads which are currently implemented as flat file transfers directly to the staging server file system would need to be designed and built from scratch.

3.4.8.7 Summary

As a repository of justice-related information for the purpose of providing analysis for the needs of the Iowa Justice community, the current interfaces and operations of the Justice Data Warehouse meet those needs. However, for CJJP to interface with systems that are service-oriented and transaction-based in their data exchange processing, the JDW would need to be enhanced to accommodate receiving data in that context. Rather than monthly batch loads, it is feasible that data would be sent to the JDW real-time as part of an overall workflow. Exposing web services, working with Teradata to handle XML structured data, and updating the technologies of the current staging environment are possible approaches for the JDW to participate fully in a workflow-driven, transaction-based environment for exchanging data. The extent to which these changes need to be made will be dependent on the extent to which the JDW is expected to participate in data exchanges real-time as opposed to monthly updates.

3.4.9 Iowa Communications Network

The Iowa Communications Network (ICN) is an independent agency of the Executive Branch providing telecommunication services a legislatively authorized customer base. Oversight of the ICN is provided by the Iowa Telecommunications and Technology Commission (ITTC), a five-member body authorized by the Iowa Legislature and an Executive Director.

The ICN is legislatively authorized to provide these services to Iowa Executive Branch agencies, the Judicial Branch, federal agencies, public libraries, and education institutions (public and private). Customers with a limited access to service include hospitals and physicians whom can only use the video and data services offered by ICN.

The agency is specifically precluded by Iowa law from providing service to local city and county governmental entities. An attempt to make the ICN available to this customer base was unsuccessful in the 2005 Legislative Session. The main opposition to the expansion of service was from the private industry providers, believing it to be unwarranted competition to their own service offerings. However, the ICN does have a presence in all 99 counties mainly into the local law enforcement agencies and/or the courts. All of these connections are paid for by the Department of Public Safety or the Judicial Branch, both of which are authorized subscribers to ICN services.

3.4.9.1 Services

The agency can be best described as a full service telecommunications provider, maintaining 3,300 miles of fiber optic lines in Iowa. Among the services they offer are:

- Phone/Voice
- Data
- Video
- Internet

The network has a reliability rating of 99.999%.

3.4.9.2 Security

For customers with ICN services to the Internet, the agency will offer to place a firewall between the ICN connection and the Internet. Currently all executive agencies are using this service. Additionally, the Department of Corrections employ firewalls in addition to those provided by the ICN. The Judicial Branch connections utilize their own firewalls and ICN does not provide any additional filtering. Agencies can place their own security measures across the network, such as VPN, SSL and encryption, but the ICN does not currently offer these security measures to the customer base.

3.4.10 Information Technology Enterprise

The Information Technology Enterprise (ITE) is one of four enterprises with the Department of Administration. ITE provides a variety of information technology related services to the Iowa State Government. The Enterprise's primary responsibilities include:

- Developing and implementing recommended standards

- Developing and maintaining security policies and systems
- Coordinating the acquisition of information technology by participating agencies

The organization is headed by the ITE Chief Operating Officer (COO), who also serves as the Department of Administration Chief Information Officer (CIO). Currently the COO and the Executive Director of the ICN positions are both being performed by a single resource. Oversight of the enterprise is provided by four different councils:

- Technology Customer Council
- Information Technology Council
- IOWAccess Advisory Council
- State of Iowa CIO Council

The 2005 Iowa Legislature replaced the Information Technology Council with the Technology Governance Board (HF839) which takes effect July 1, 2005.

ITE currently manages roughly 30% of the state infrastructure. The Department of Human Services and Department of Revenue are the Enterprise's largest customers, but other executive agencies are served by the organization.

3.4.10.1 Services

The ITE provides services related to the delivery and maintenance of information technology for state government agencies. Some of the most critical functions provided by ITE are development and implementation of recommended standards, development and implementation of security policies, delivering information technology services related to the design, operation support and hosting of information technology solutions.

The Enterprise is in the early stages of developing recommended standards. These evolving enterprise IT standards will address the recommended platforms for hardware, software applicable to the PC, mid-tier application and enterprise application. Enforcement of these standards for participating agencies, and assistance procuring compliant solutions will be part of the ITE IT Standards program.

The Enterprise also offers a variety of consulting IT services to participating state agencies, and provides published rates for them. Services currently offered by the ITE include:

- Mainframe Services
- Network Services
- Web Services
- VPN (Virtual Private Network) Services
- Server Farm Services
- SING System Access
- Business Objects and Data Warehouse (Teradata)

- Server Usage Support (Database/Internet)
- Electronic Information Management
- Enterprise Server Backup Services Special Handling
- Enterprise LAN Support and Desktop Management
- Enterprise E-mail Services
- Help Desk and DeskTop Services
- Training and Multimedia Services
- Security Services
- Storage Area Network (SAN) and Related Services
- Rates for ITE Personnel
- Rates for Purchased Consultation

3.4.11 County Attorney

The prosecution of criminal charges is handled in Iowa by the County Attorneys. There is an elected County Attorney in each of the 99 counties in Iowa. To gather information for this As-Is Technical Assessment, three approaches were used:

1. The County Attorneys were asked to respond to a survey created to measure their current or near-term utilization of technology to support their day-to-day business processes.
2. A teleconference interview with the Project Manager of the Iowa County Attorneys Case Management Project was conducted.
3. Previous studies of the state of the County Attorney's technical capability were reviewed. This included a SEARCH Technical Assistance Report completed in January of 2002,[23] and a CJJP examination completed in October of 2002.[24]

The breadth of different technical environments among Iowa's County Attorney offices is quite extensive. The differences can typically be drawn between the rural and urban areas. Of the 99 offices, 49 of them are still served by a part-time County Attorney. The lack of automation in the County Attorney offices was cited as a major barrier by SEARCH to the ability of Iowa achieving end-to-end full statewide integration. Since that report, the County Attorneys have worked towards removing that barrier by creating the Iowa County Attorneys Case Management Project. The project has worked towards the selection of a common prosecutor case management system to be available at any Iowa County Attorney's office that chooses to participate. Two different applications are being made available through the project: (1) ProLaw from Thompson Elite and (2) Judicial Dialogue from Judicial Dialogue Systems. The number of participants has

[23] Iowa Integration Technical Assistance, Lawrence P. Webster, January 28, 2002.
[24] Examination of the Level of Computer Utilization for Management Purposes, Software Usage by Title and the Availability of Existing Communication Systems in County Attorney's Offices and County Jails in Iowa, Terry L. Hudick, October 2002.

fluctuated over the course of the effort, but the 13 participating counties were prepared to test and implement their solution by the end of June 2005. However, the door is still open for other counties to join the effort, and it is expected that an early success of the project will lead others to join as well. A thirteenth County Attorney office is also expected to be implemented in the near future, but not in the initial roll-out of the application. The agencies that are participating in the project are listed below.

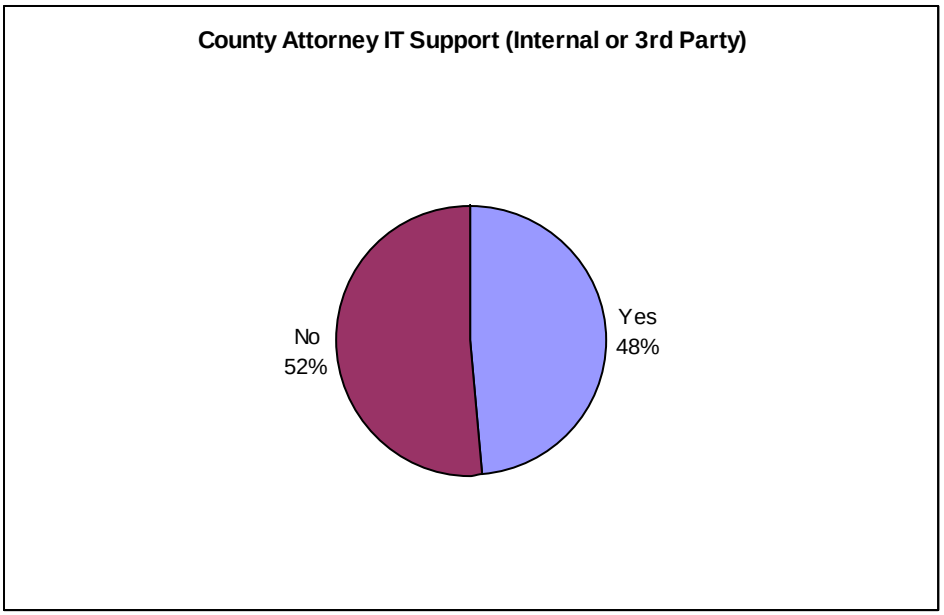
Iowa County Attorneys Case Management Project Participants	
Butler County Attorney	Johnson County Attorney
Carroll County Attorney	Madison County Attorney
Dallas County Attorney	Muscatine County Attorney
Dubuque County Attorney	Plymouth County Attorney
Guthrie County Attorney	Pottawattamie County Attorney
Hardin County Attorney	Tama County Attorney
Henry County Attorney	

Several agencies also responded to the technical assessment survey made available via the web. In total, 32 agencies responded to the web survey. The agencies that participated are listed below.

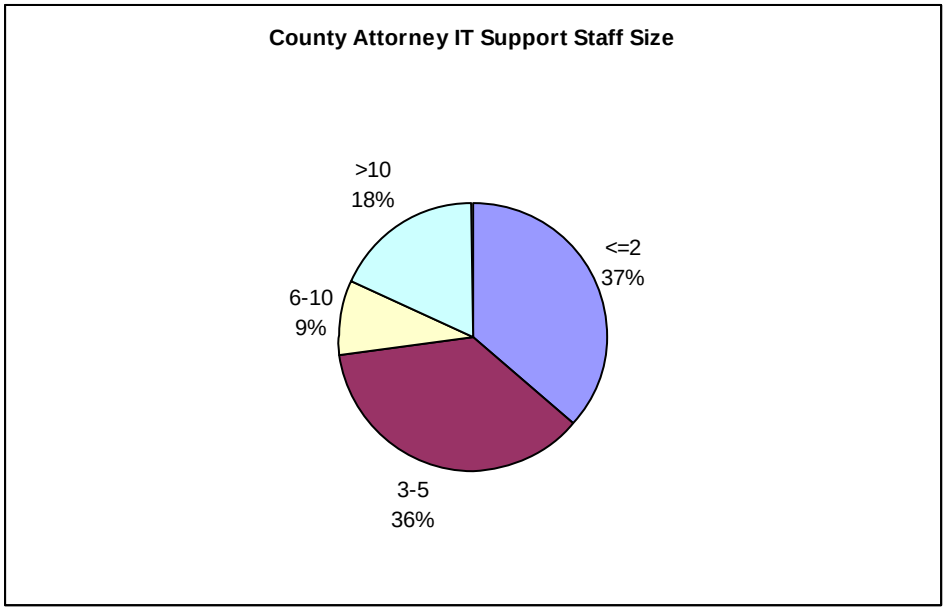
Iowa County Attorneys Survey Participants

Black Hawk County Attorney	Lee County Attorney
Boone County Attorney	Linn County Attorney
Bremer County Attorney	Lucas County Attorney
Butler County Attorney	Madison County Attorney
Calhoun County Attorney	Mahaska County Attorney
Cedar County Attorney	Osceola County Attorney
Clarke County Attorney	Plymouth County Attorney
Clay County Attorney	Pocahontas County Attorney
Crawford County Attorney	Pottawattamie County Attorney
Des Moines County Attorney	Ringgold County Attorney
Dubuque County Attorney	Tama County Attorney
Emmet County Attorney	Union County Attorney
Hardin County Attorney	Van Buren County Attorney
Iowa County Attorney	Warren County Attorney
Jefferson County Attorney	Winneshiek County Attorney
Jones County Attorney	Wright County Attorney

Of the County Attorney offices that did respond or information could be gathered from, almost half (52%) have some IT support staff provided from either internal resources or from a third party via contract.

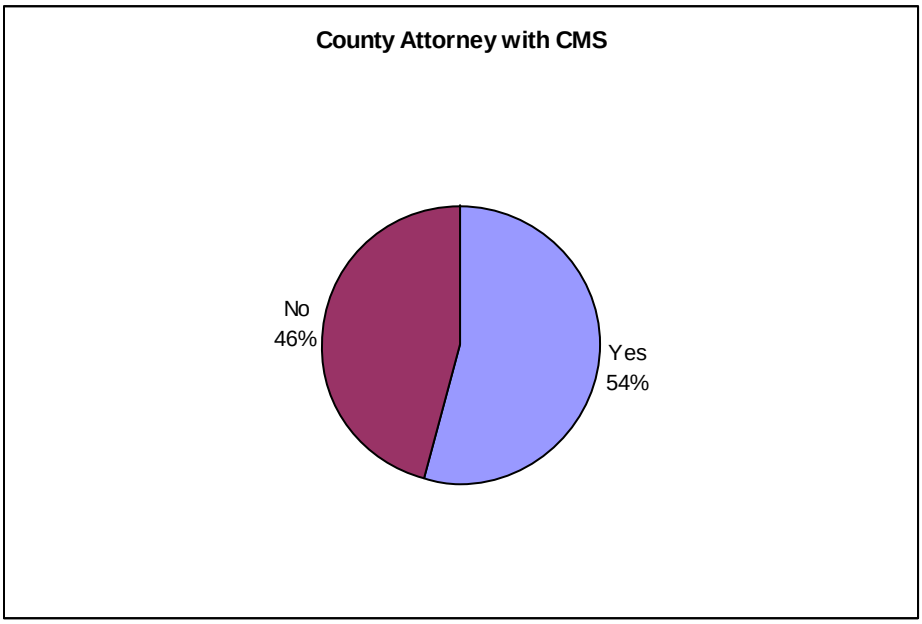


The support staff in the offices that have IT support vary between two or less and more than 10. The larger staffs are not as typical however, with over 70% of the offices having 5 or less IT support staff, as illustrated in the graph below.

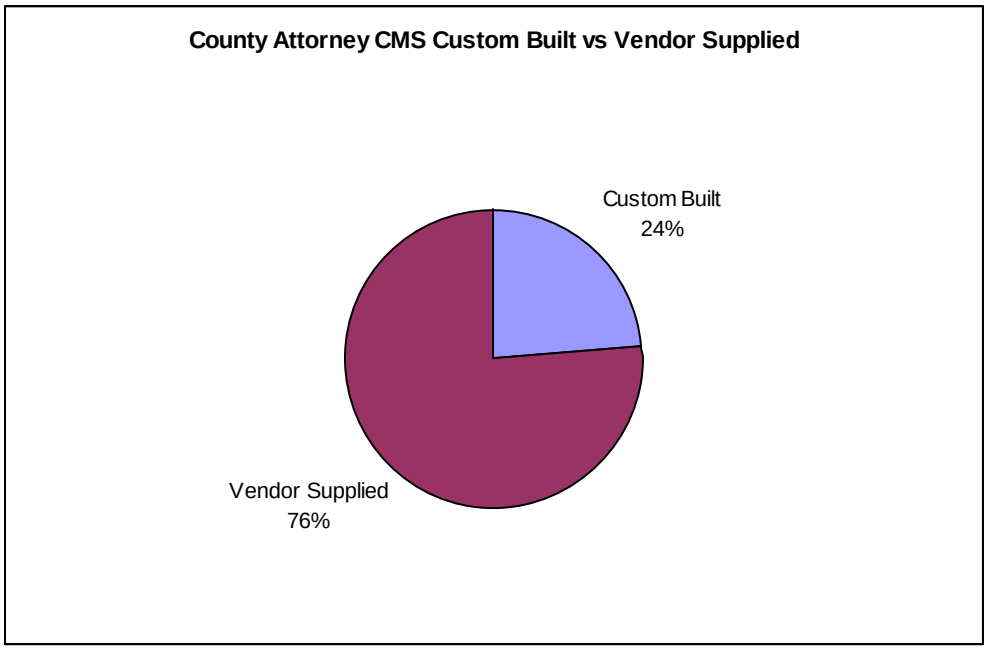


3.4.11.1 Current Systems Environment

The number of County Attorneys' Offices that are currently using a case management system, or have plans to implement one in the next 18 months, is again almost half. Information was received from 21of the 39 offices (54%) indicating the offices were already using or were very close to implementing a technology system to help in the business management of their case load. This finding is an increase of approximately 7% over the percentage of agencies using automated systems in the 2002 CJJP study and demonstrates the County Attorneys' work toward overcoming the barrier cited by SEARCH in January of the same year.



The County Attorney offices show a preference for vendor COTS solutions over their own custom built systems by a 3-to-1 margin. Sixteen of the 21 respondents were using COTS tools in their implementations.



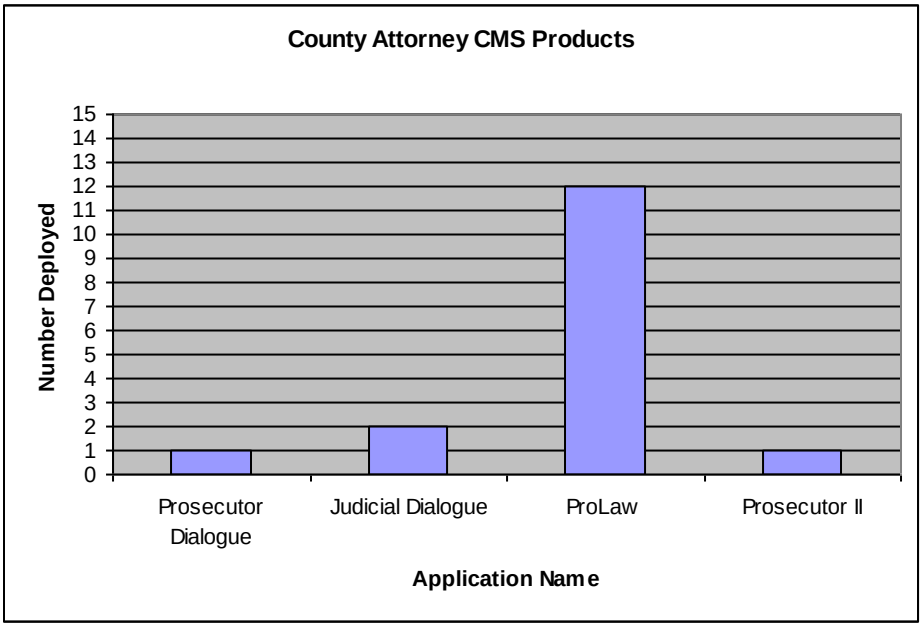
The Iowa County Attorneys Case Management Project is having a significant impact on the COTS solution of choice in a given prosecutor's office. While the project has selected two different applications to make available through its endeavor, both ProLaw and Judicial Dialogue, the selection of ProLaw has been the overwhelming choice. It surpasses its closest competitor by 10 implementations and has 12 of the 16 vendor-provided systems identified in Iowa.[25] This trend is a reversal from the 2002 CJJP study which found Prosecutor Dialog as the solution of choice for a CMS, with almost 30% of the implementations at that time (14 total). Of the 12 Prolaw implementations being handled by the Iowa County Attorneys Case Management Project:

- Five of them are being deployed to agencies that had no CMS system in 2002
- Four of them are replacing Prosecutor Dialog applications
- Three are replacing systems other than Prosecutor Dialog

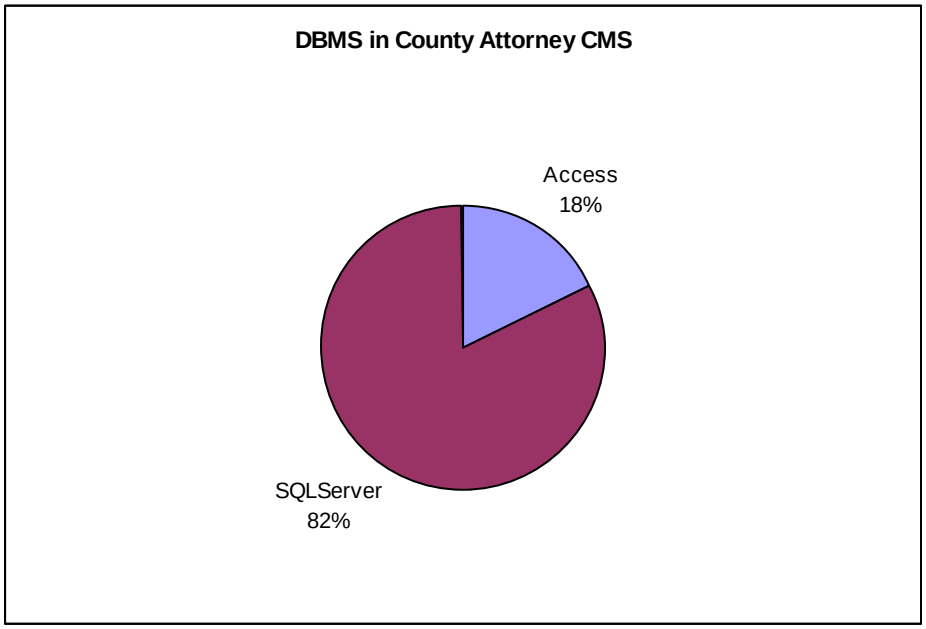
The following bar graph depicts the documented responses to the survey or the interview with the Iowa County Attorneys Case Management System Project Manger. She anticipates that at least nine other implementations of Prosecutor Dialog in Iowa, as well

[25] It is important to note that some applications in production in Iowa County Attorney offices are not represented in this graph because of their near-term replacement by ProLaw.

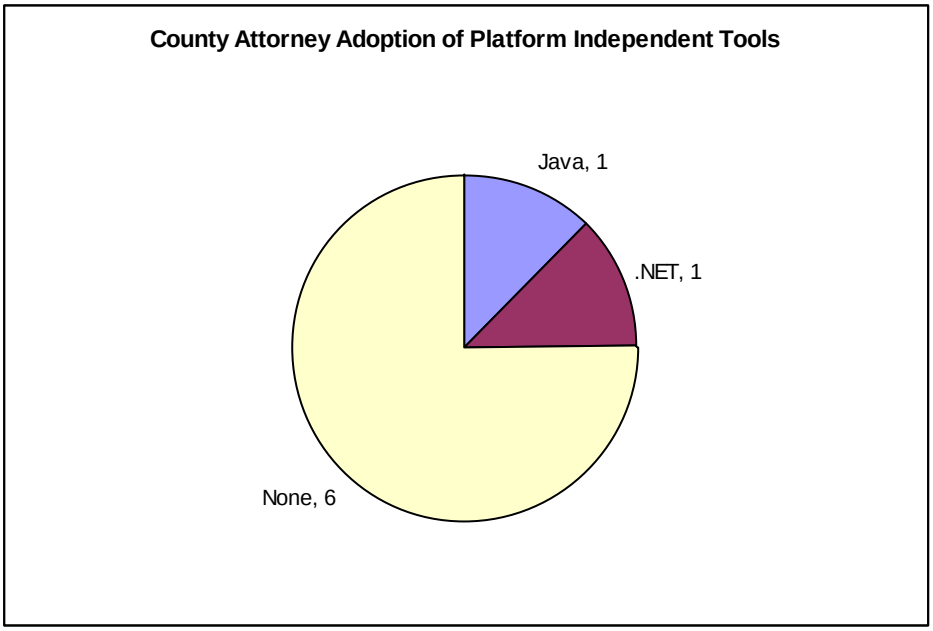
as other CMSs actively being implemented in Iowa County Attorney offices. However, they could not be verified in this effort and are not included in the result set.



When comparing the persistent data storage platforms used in both vendor and custom built applications, SQL Server dominates the field with 82% of the identified systems operating on that RDBMS platform. A distinct second choice is Microsoft Access with the remaining 18%.

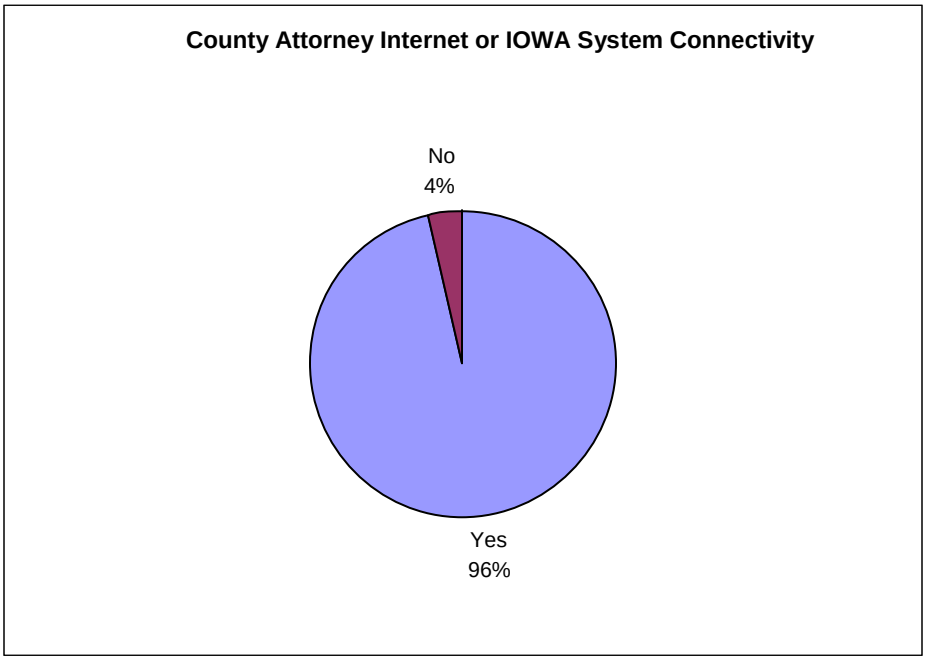


The County Attorney offices are not implementing platform-independent tools such as Java and .NET at a rapid pace. When asked what the plans were for the implementation of such platforms, only eight offices responded to the question in the survey, and only two indicated that they either were using them or would be in the next 18 months.

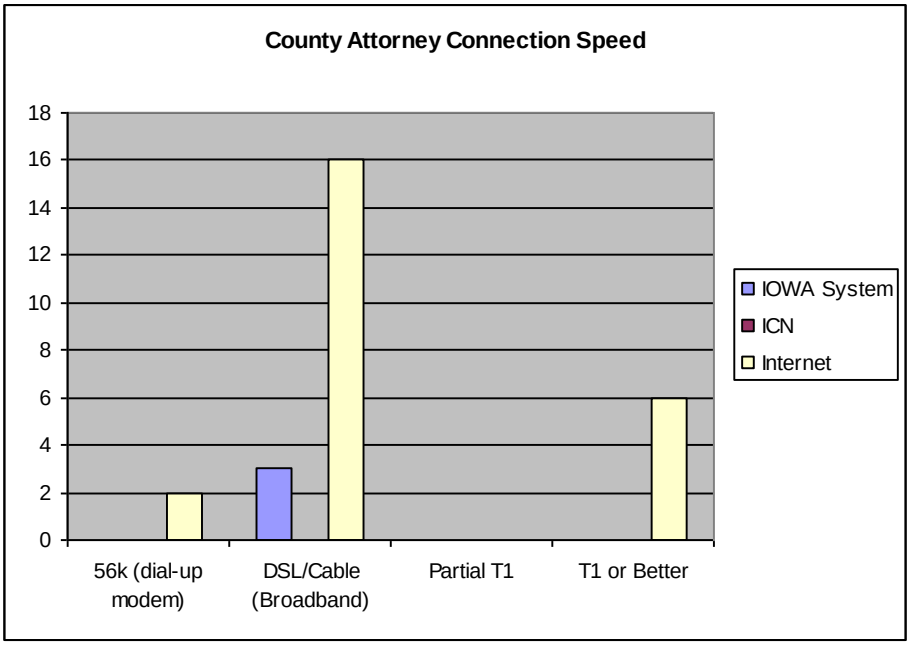


3.4.11.2 Network Connectivity

The County Attorney offices maintain a high rate of connectivity to at least one of the major communication infrastructures in Iowa. When asked if their agency maintained connectivity to the IOWA System, or the Internet, 96% of the agencies that responded to the survey indicated "Yes." Only one County Attorney office in 27 answering the technical assessment survey responded "No."

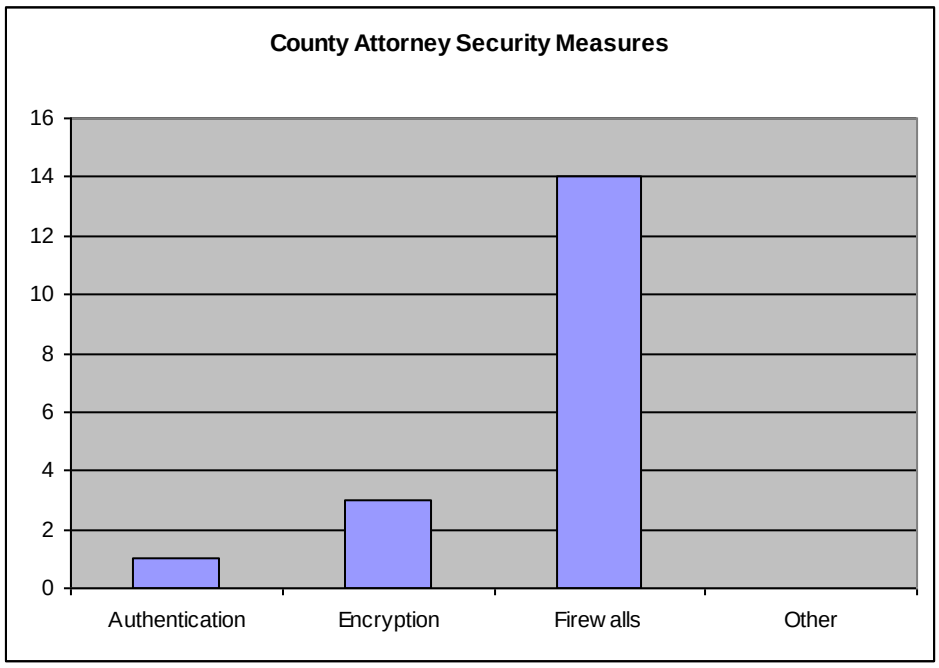


In addition to establishing the connectivity rate, the survey also captured the specific trends indicating how County Attorney offices are connected. The survey revealed not a single respondent maintains any connection to the ICN network, as local governments in Iowa do not have access to the ICN. A broadband or high connection to the Internet dominates the communication infrastructure of choice in the respondents with 22 of the 27 connections utilizing that model. Only two respondents had less than a broadband Internet connection. Three offices that maintain a broadband connection to the Internet also maintain a broadband connection to the IOWA System as shown in the figure below.



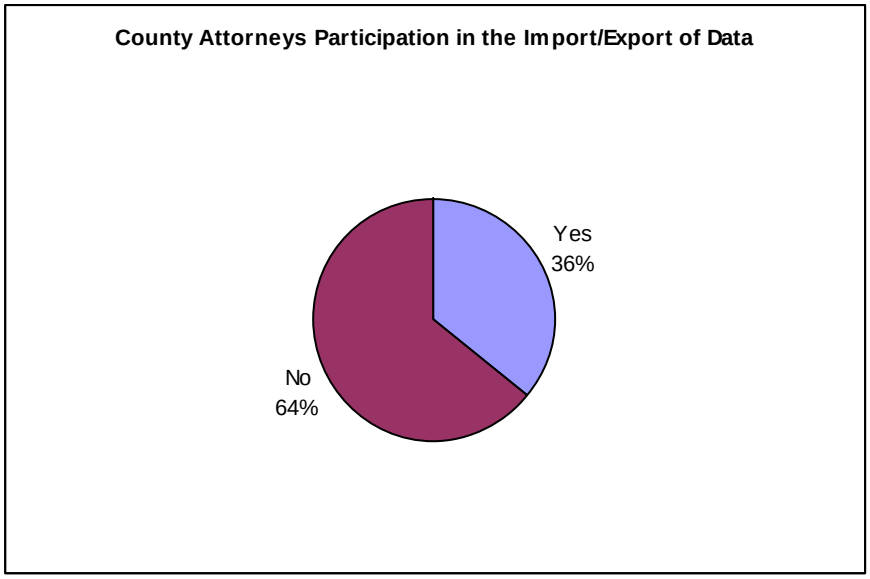
3.4.11.3 Current Security Policies

County Attorneys responding to the survey were asked what type of security they were utilizing in their applications and networks to protect the information in their applications. The implementation of a firewall is fairly prevalent in the prosecutor offices, with minimal use of encryption or authentication. The following bar graph depicts all of the 18 responses received from the County Attorneys to this question.

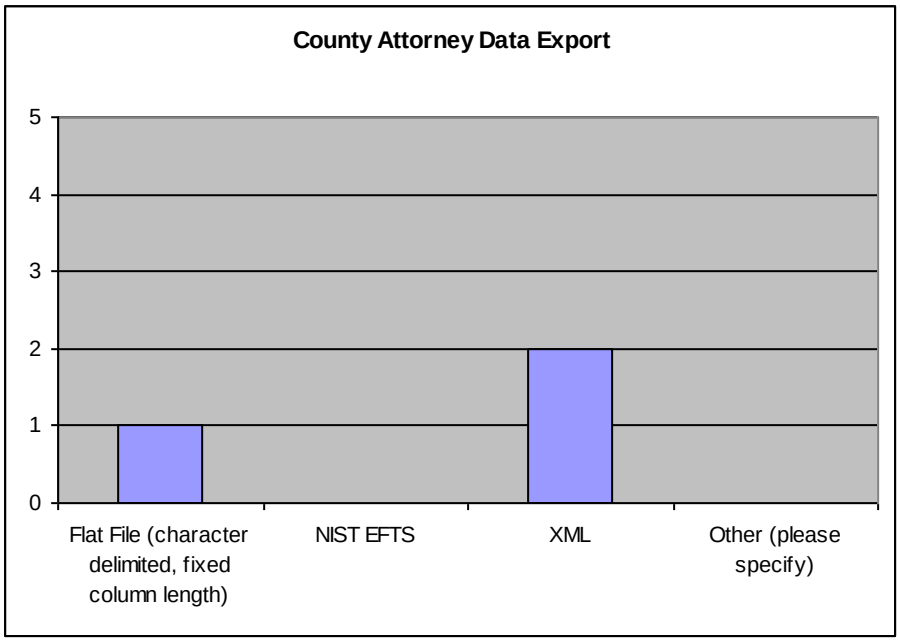


3.4.11.4 Data Standards

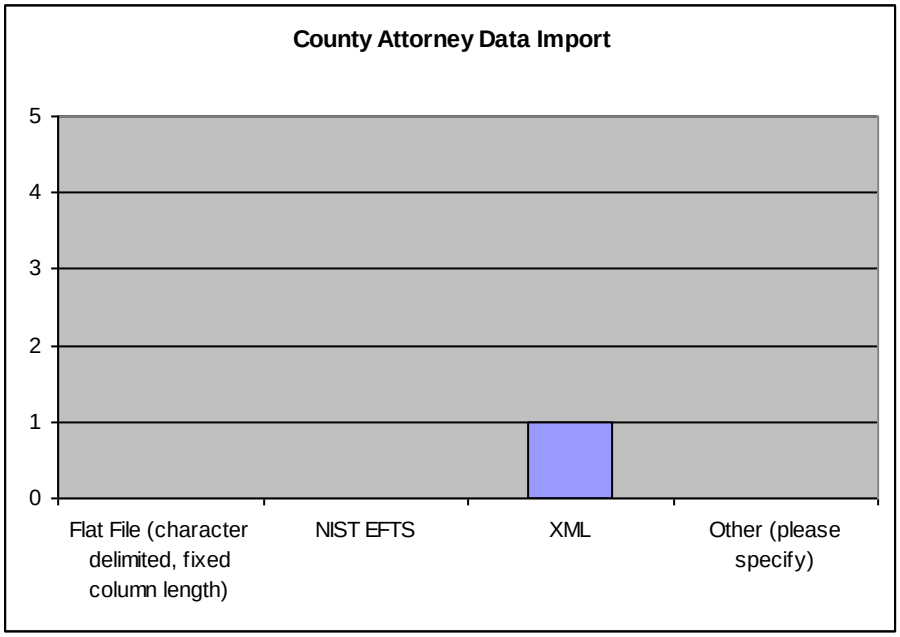
As a group, the Iowa County Attorneys are not participating in large numbers in information exchange interfaces. Ten of the 28 respondents answering a question about their importing or exporting of data from their systems indicated "Yes." Only half that number (5) indicated what type of file structure they were using to achieve the information exchange. However, the utilization of XML and GJXDM-compliant schema for information exchange is the next major phase of the Iowa County Attorneys Case Management System Project, and the numbers presented here are expected to change dramatically if the funding can be found to pursue the creation of the standards and infrastructure necessary to share information in a standardized manner with the County Attorney partner agencies.



The respondents who indicated they were exporting data from their systems for use by an external application stated they were using XML (two offices) or a flat file format (1 office) to achieve the exchange.



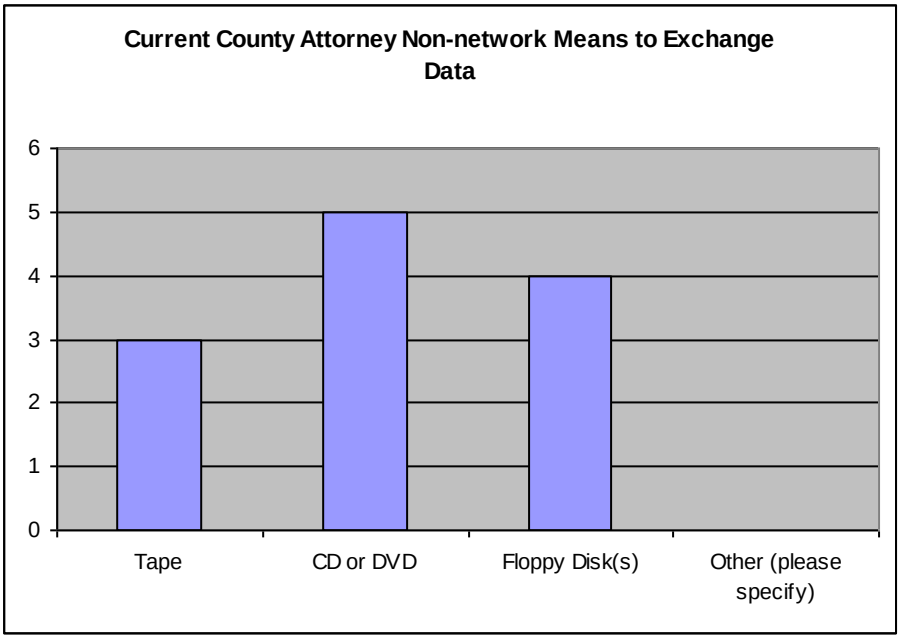
For importing data, there was only one response received of the 32. The structure the imported data was being provided for use was identified as XML.



3.4.11.5 Transaction Processing Capability

The use of a guaranteed messaging solution in the sharing of information by Iowa County Attorneys has not yet begun to materialize. Not one of the respondents identified the use of MQ Series, JMS, or WS-Reliability in their current technology architectures for event-driven transaction exchanges.

Several agencies indicated that they relied on non-network media for the exchange of data either into or out of their applications. Respondents identified tape (3), CD or DVD (5), or floppy disks (4) in almost equal numbers.



3.4.11.6 Adoption of Web Service/SOA Standards

The creation of service-oriented architectures and web services is not a major technological initiative in the current County Attorneys deployments. Only two of the respondents indicated the use of SOA technology such as SOAP and XML schemas in their near-term future environments. It is expected that Phase 2 of the Iowa County Attorneys Case Management System Project, if properly funded, could impact the number of agencies using SOA principles and architectures in their information sharing projects.

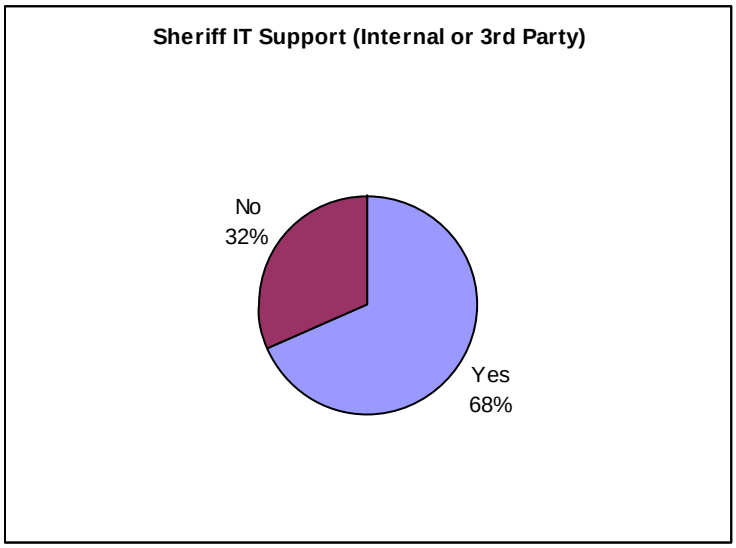
3.4.12 Sheriff Offices

There are 99 Sheriff Offices in the State of Iowa – one in each county. A survey to gather information from this geographically dispersed group was developed and made available via an Internet web site. All 99 Sheriff Offices were invited to participate in the information gathering process. Of that number, 29 responded to the As-Is Technical Assessment portion of the survey. The participating Sheriff Offices are listed below.

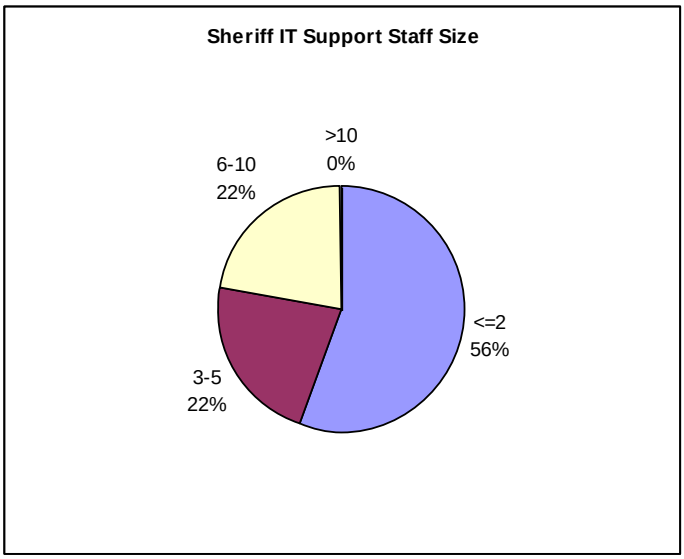
Participating Sheriff Offices	
Adams County Sheriff's Office	Montgomery County Sheriff's Office
Audubon County Sheriff's Office	O'Brien County Sheriff's Office
Calhoun County Sheriff's Office	Pottawattamie County Sheriff's Office
Cerro Gordo County Sheriff's Office	Poweshiek County Sheriff's Office
Chickasaw County Sheriff's Office	Sac County Sheriff's Office
Clayton County Sheriff's Office	Scott County Sheriff's Office
Clinton County Sheriff's Office	Sioux County Sheriff's Office

Participating Sheriff Offices	
Dallas County Sheriff's Office	Story County Sheriff's Office
Dubuque County Sheriff's Office	Warren County Sheriff's Office
Floyd County Sheriff's Office	Winnebago County Sheriff's Office
Grundy County Sheriff's Office	Woodbury County Sheriff's Office
Hancock County Sheriff's Office	Henry County Sheriff's Office
Jasper County Sheriff's Office	Polk County Sheriff's Office
Mahaska County Sheriff's Office	Jones County Sheriff's Office
Monona County Sheriff's Office	

Of the Sheriff Offices that did respond to the survey, 68% indicated that they had an IT support staff. This staff was either internal to the Sheriff Office, provided through a contract from vendor, or a combination of the two.

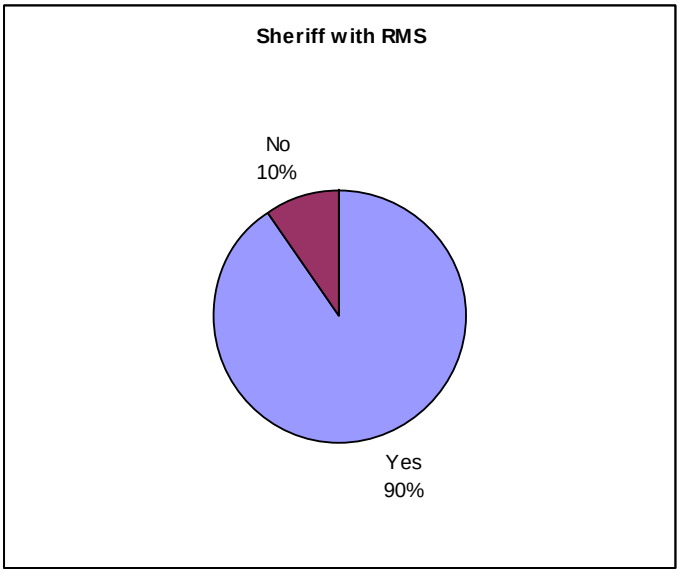


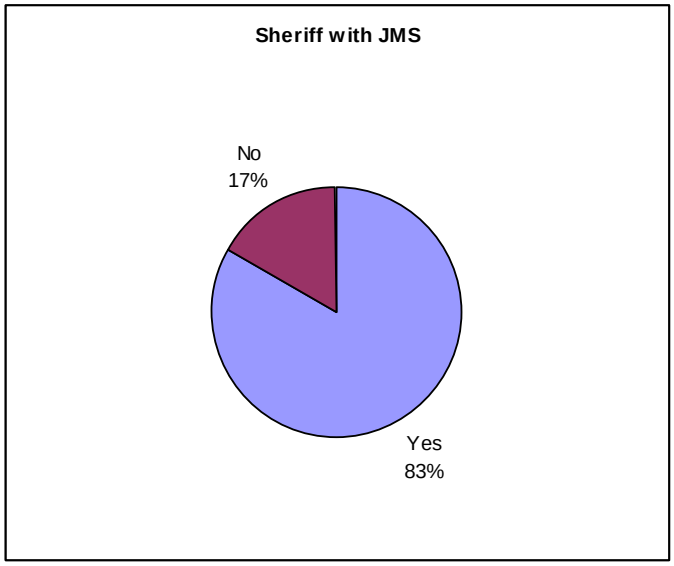
The size of the staff was typically one or two people 56% of the time and the other 44% having a staff between three and 10 persons. None of the responding Sheriff Offices have a staff larger than 10 resources.



3.4.12.1 Current Systems Environment

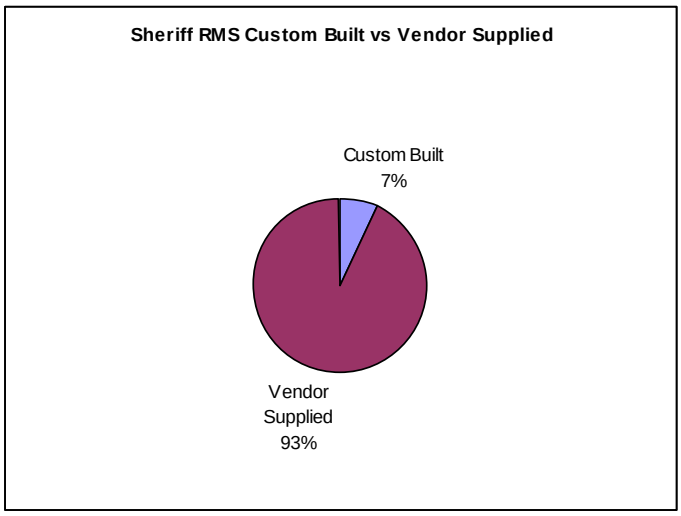
Sheriff Offices were asked to provide information related to their current utilization or planned implementation in the next 18 months of Record Management Systems (RMS) and/or Jail Management Systems (JMS) to support their business processes. Responses collected clearly show there is a high use of RMS systems (90%) and JMS systems (83%) in the Iowa Sheriff Offices. The number of jails with JMS systems is consistent with an inventory of software used in Sheriff Office jails in October of 2002 by CJJP,[26] though the percentage of use is slightly lower (1.4%) in the more recent survey.

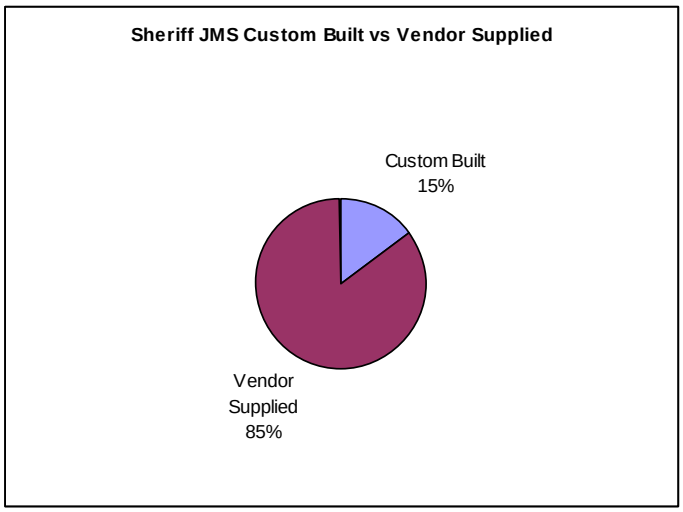




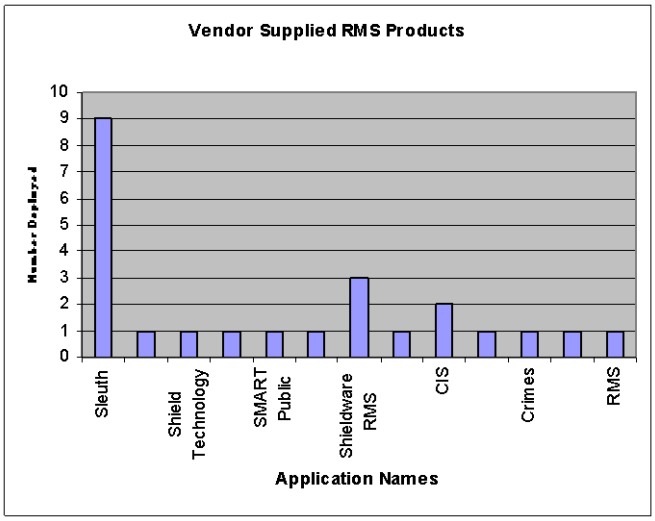
[26] Examination of the Level of Computer Utilization for Management Purposes, Software Usage by Title and the Availability of Existing Communication Systems in County Attorney's Offices and County Jails in Iowa, Terry L. Hudick, October 2002.

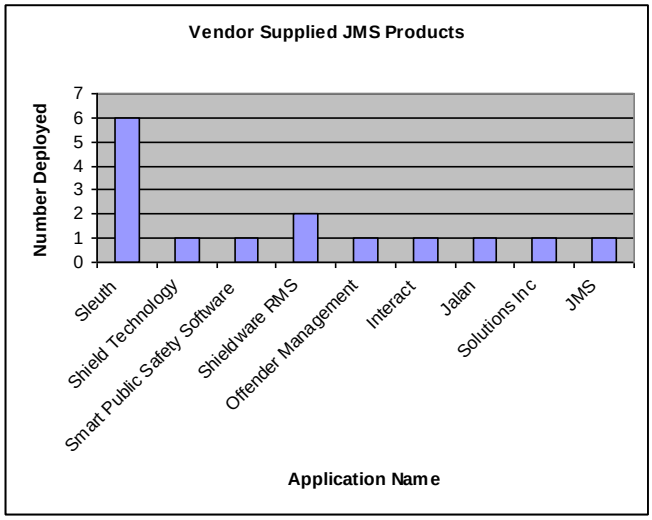
The respondents also had a clear choice of using vendor supplied COTS applications over a system that was custom built for them. Of the 28 offices using a RMS system, 26 of them were using a vendor supplied tool. The number of JMS installations by vendors was 17 of the 20 identified.



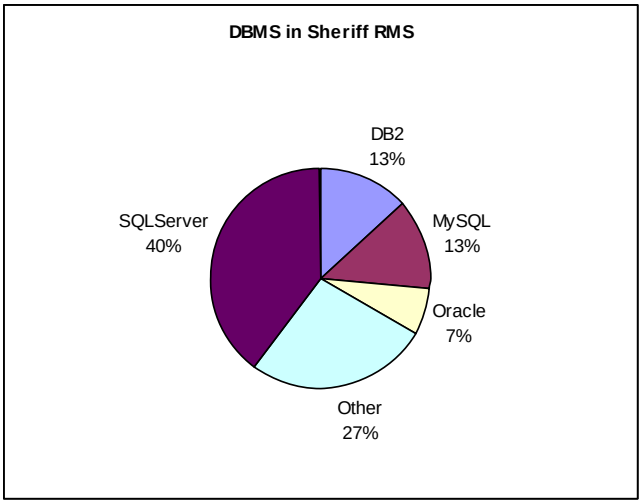


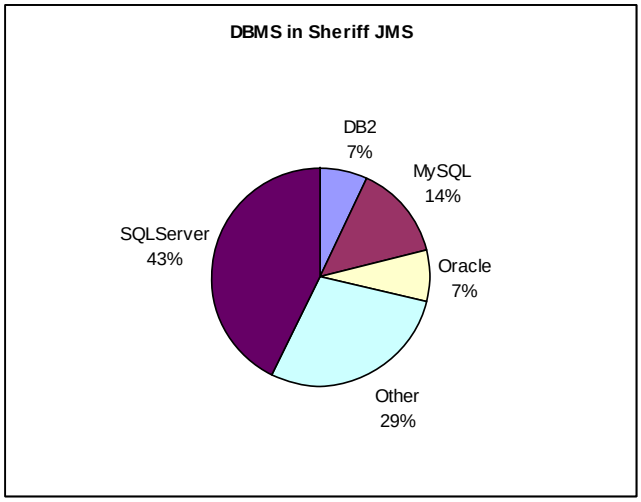
The Sheriff Offices also demonstrated an overwhelming preference of an RMS and JMS COTS tool. Both categories were heavily dominated by the use of Sleuth Software. In the RMS category, Sleuth was used by 38% of the agencies. In the JMS category, it had 40%. This finding is again consistent with the earlier inventory of software used in Sheriff Office Jails by CJJP in 2002. The names of each vendor supplied RMS and JMS tools and the number deployed in respondents' systems are depicted in the bar graphs below.



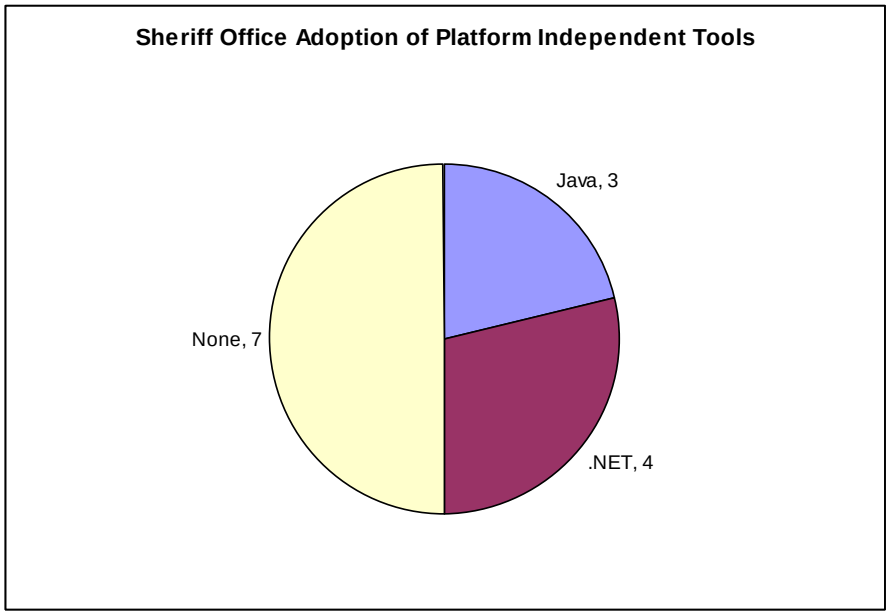


DBMS servers utilized for persistent data storage in both vendor supplied and custom build applications were predominantly SQLServer and the "Other" category. Agencies with Sleuth software responded in either one of these two categories, making it unclear if the solution comes standard with a SQLServer database, used a database not available in the survey list, or had a proprietary storage system in some deployments. Research at the software provider's website indicated that the platform could be deployed to multiple databases. All of the database types are listed in the following pie charts:



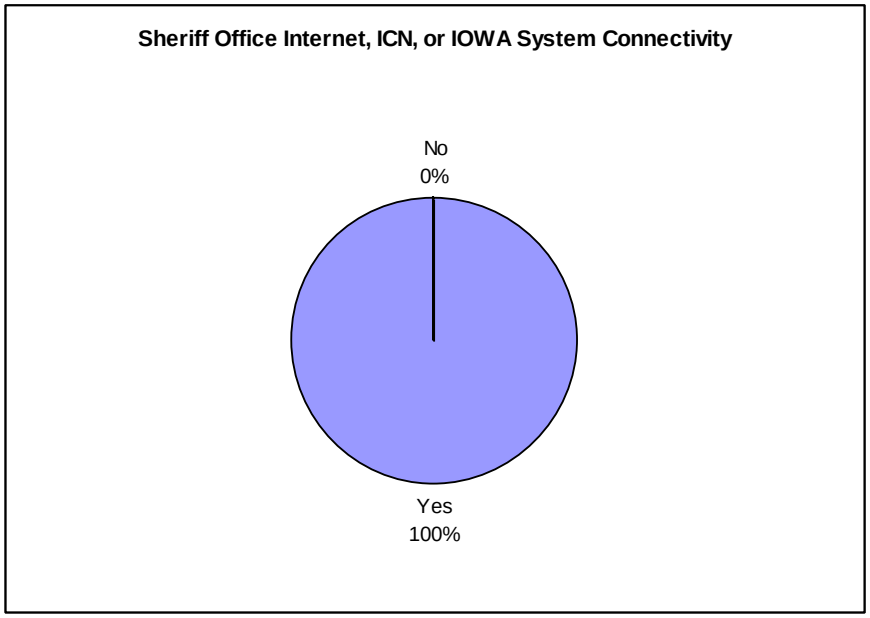


Only 14 of the Sheriff Office respondents replied to the inquiry of their use of platform independent tools such as Java or .NET. The responses indicate that there is about a 50% utilization of these technologies within the agencies. Seven Sheriff Offices indicated that they were using these types of platforms. The exact implementation is depicted in the pie chart below.

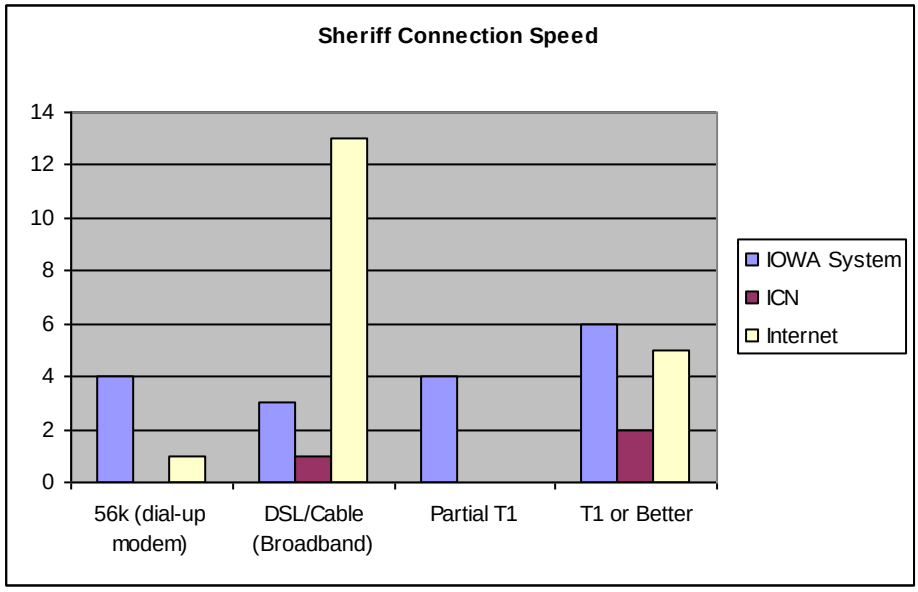


3.4.12.2 Network Connectivity

Connection to a communication networks such as the IOWA System, ICN or the Internet was 100% for the Sheriff Offices responding to the survey. Every office had the ability to connect to one of these major communication networks, and some were accessing multiple networks. The 2002 study of the jails in Iowa found that 90% of those facilities had some connection to one of these three communication structures.

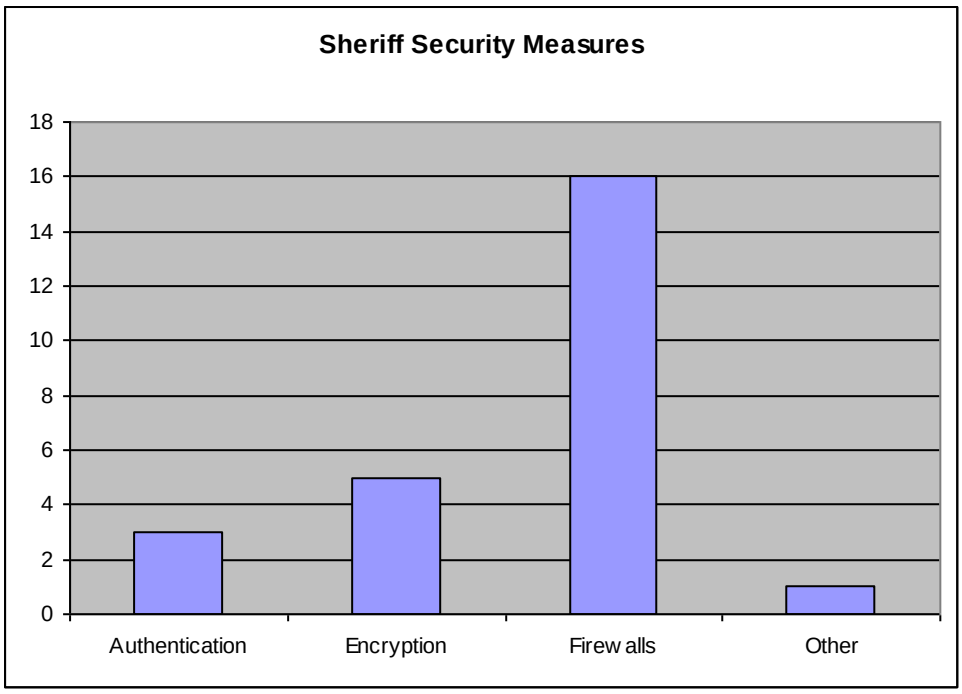


Connection speeds to the networks varied from 56k dial-up to dedicated T1 or better. The most common connection in the Sheriff Offices was a broadband connection (DSL or Cable) to the Internet. The exact number of each connection speed to the identified communication structure is depicted in the bar graph below.



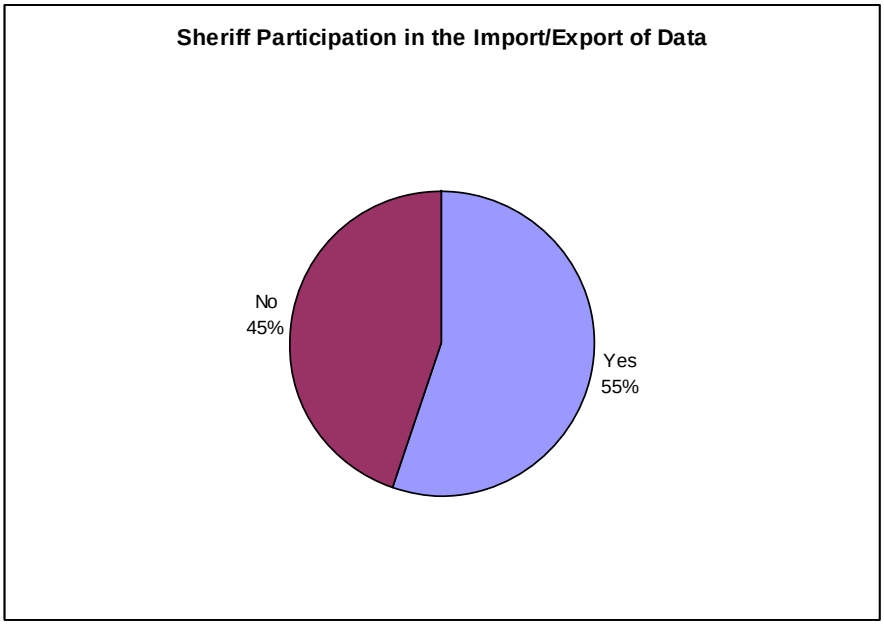
3.4.12.3 Current Security Policies

The Sheriff Offices were asked about the use of security measures in their applications and network infrastructure. Each was asked if they utilized authentication, encryption, firewalls or any other method to help secure there data and network traffic. Six agencies were using more than one of the technologies asked about. The one "Other" response received in the results was the use of bio-key technology. The following bar graph depicts the responses received from the local law enforcement agencies.

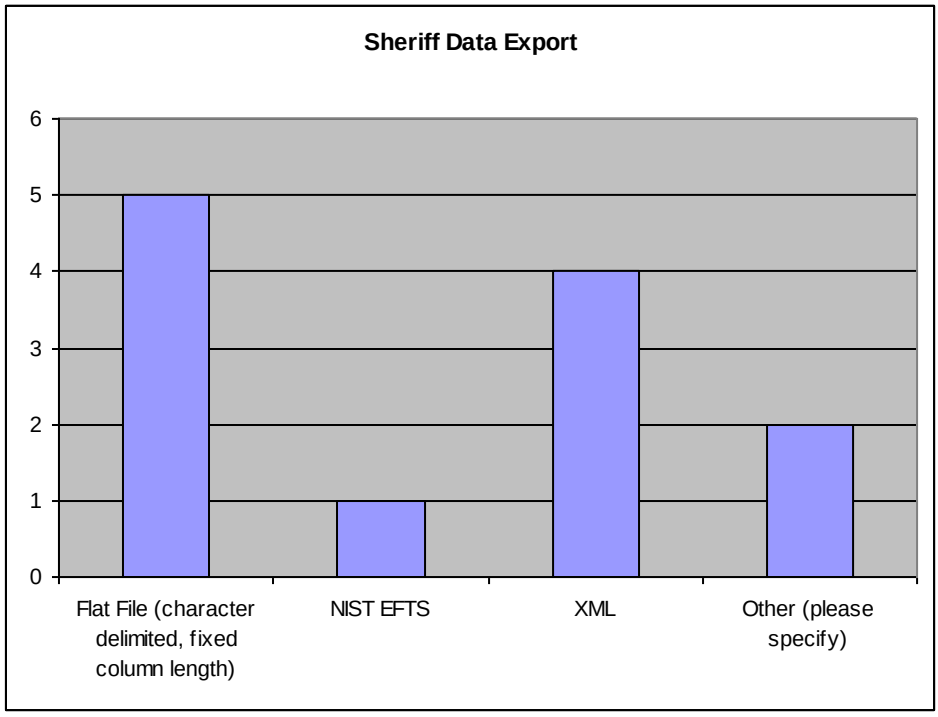


3.4.12.4 Data Standards

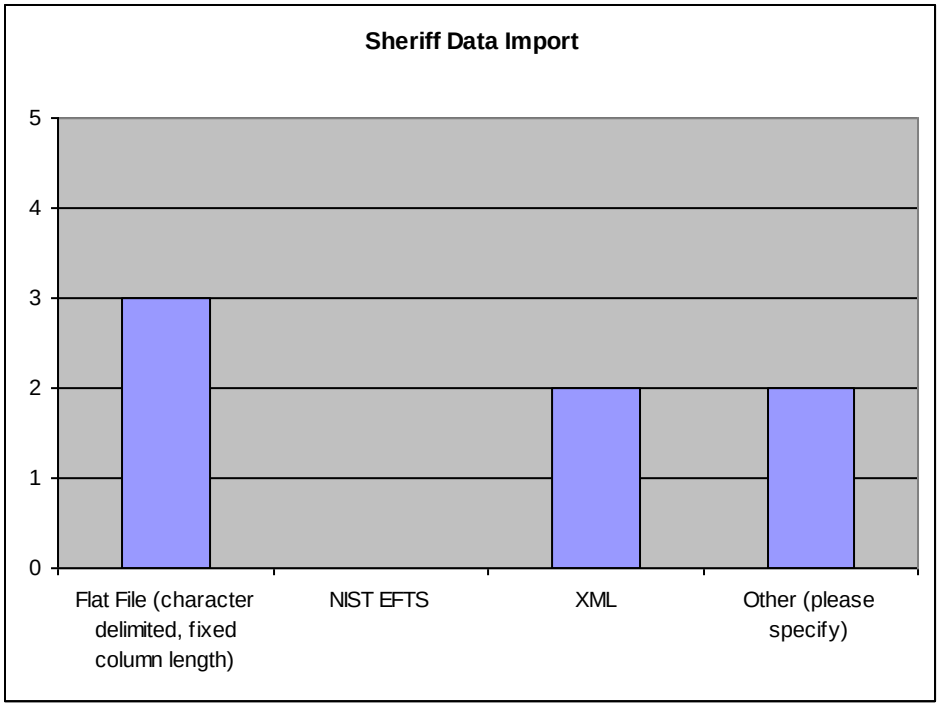
Over half of the Sheriff Offices are currently sharing data with other agencies in their business processes. The departments were asked if they were currently importing or exporting data between an internal or external system; 55% of the responding offices indicated "Yes."



Sheriff Offices that export data from their RMS or JMS systems use a variety of formats to accomplish the information exchange. The most popular was a flat file (character delimited or fixed column length data structures), but XML is also a popular choice, and NIST EFTS is used in at least one office. The selection of "Other" indicated unknown by the respondents making this choice.



The import of data is not as prevalent as exporting it in the Sheriff Office applications. There is still a broad range of formats being utilized: flat file, XML, and "Other", which again indicated an unknown format from the respondent.

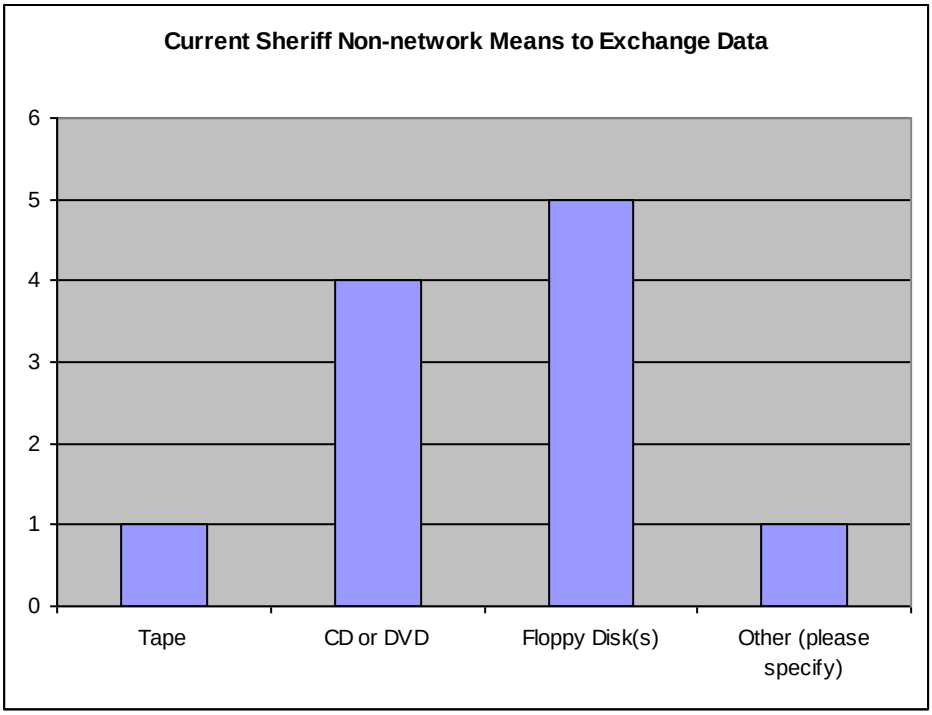


Of the agencies responding to either the import or export of data portion of the survey, five out of nine are utilizing a formal documented policy in governing what can and cannot be shared.

3.4.12.5 Transaction Processing Capability

The Sheriff Offices are not currently incorporating a guaranteed messaging model for the exchange of the information between applications. None of the respondents to the survey have implemented an MQ series, JMS, or WS-Reliability in their automated information exchange approach.

Several agencies are using non-networked medium in their information exchange (e.g., tape, CD, floppy disk). The following bar graph represents the responses received using these media. The "Other" response represents a USB Mass Storage Device.



3.4.12.6 Adoption of Web Service/SOA Standards

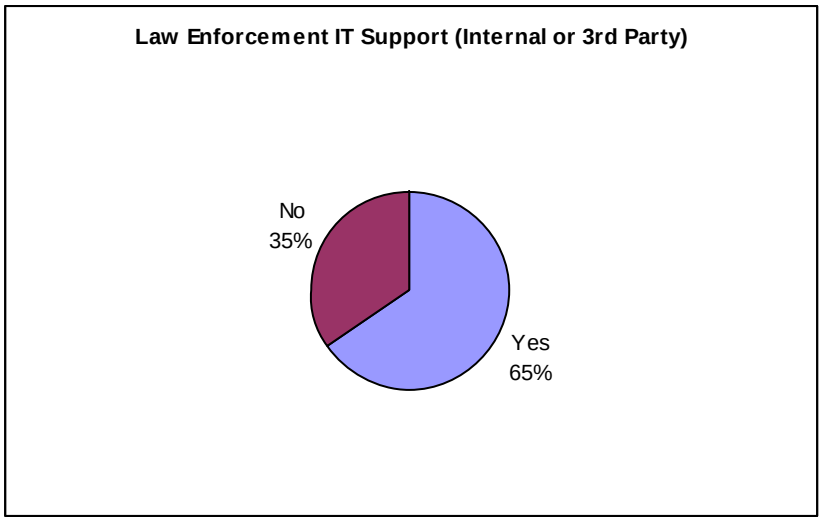
The adoption of web services and SOA architectures is an area of technology the Sheriff Offices are not implementing in large numbers. Participants were asked if they were using, or had plans to use in the next 18 months, web services, UDDI, SOAP, or XML schema. Only two respondents indicated that they were using or had plans to use web services in the time period indicated.

3.4.13 Local Police Agencies

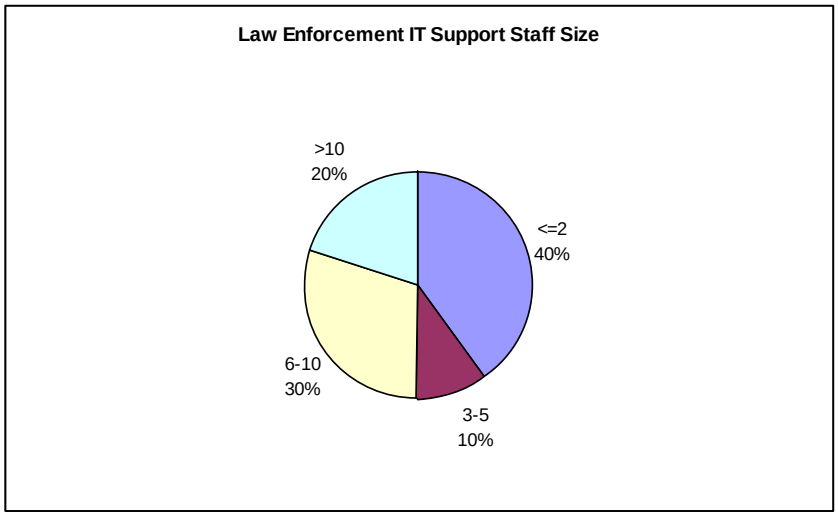
The local police departments represented the largest group of agencies that the survey tool was utilized to gather data. In total, 383 agencies were identified that could participate in the As-Is Technical Assessment. Of that number, 27 agencies did respond to some portion of the technical survey, approximately 7%. The agencies responding included the following:

Participating Police Agencies	
Albia Police Department	Le Claire Police Department
Altoona Police Department	Marengo Police Department
Ames Police Department	Mitchellville Police Department
Atlantic Police Department	Monona Police Department
Belle Plaine Police Department	Mount Pleasant Police Department
Clarinda Police Department	Nevada Police Department
Corydon Police Department	Osage Police Department
Denison Police Department	Ottumwa Police Department
Des Moines Police Department	Prairie City Police Department
Eddyville Police Department	Sheldon Police Department
Forest City Police Department	University Heights Police Department
Grinnell Police Department	Webster City Police Department
Hampton Police Department	Windsor Heights Police Department
Hawarden Police Department	

Of the agencies responding, nearly two-thirds have an IT support staff helping maintain the police agencies' technology investments. The staffing may be internal, vendor supplied, or both. Nearly half of the respondents (48%) were utilizing outside resources of some nature.

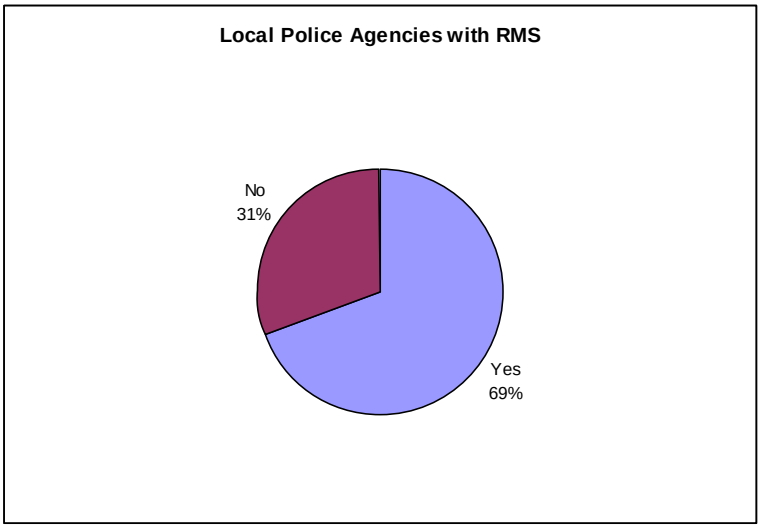


In agencies with IT support staff, the number of resources varied, with 40% having two or less, and 50% having six or more technical staff. A full breakdown of the IT Staff sizes for Law Enforcement Agencies is depicted in the following pie chart:

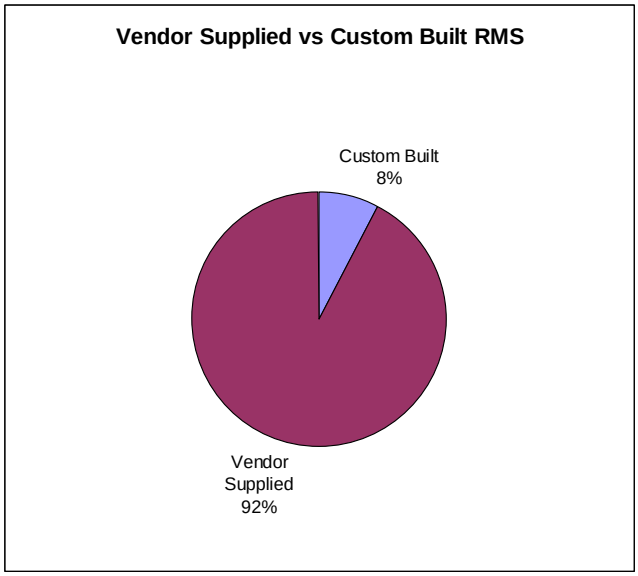


3.4.13.1 Current Systems Environment

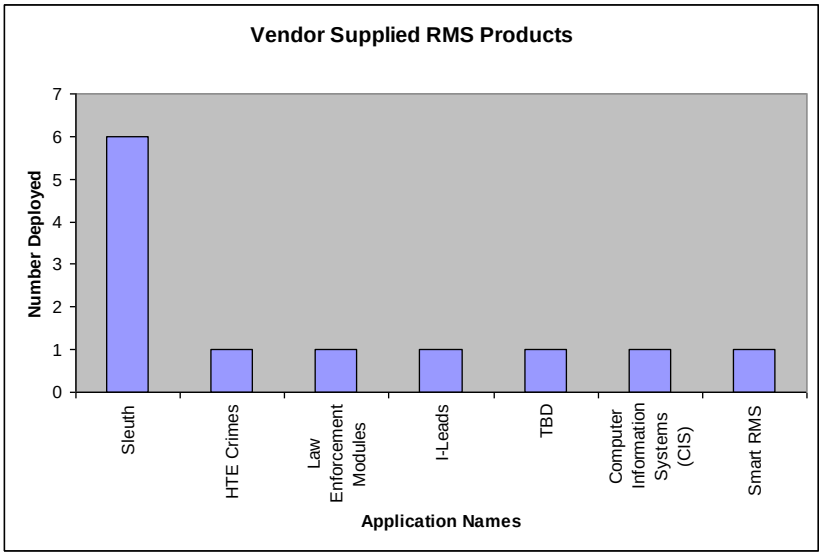
The utilization of technology to help support the records management of the local police agencies was the focus of the survey questions related to their current system environment. Of the agencies responding to a question of whether or not they used a Record Management System (RMS) or planned to implement one in the next 18 months, 18 of the 27agencies replied "Yes."



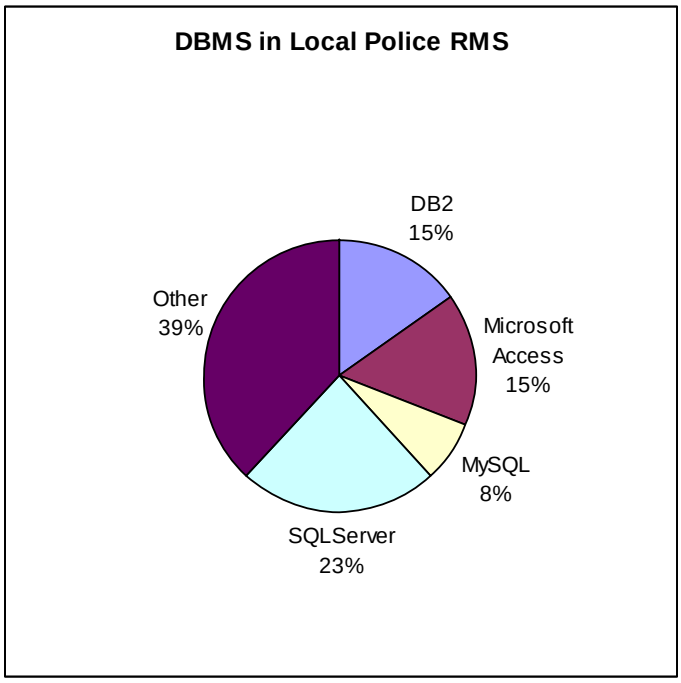
Overwhelmingly, the agencies that are using RMS systems are acquiring COTS solutions over custom-built applications. Of all the responses received, only one agency indicated that it was using a custom-built RMS application.



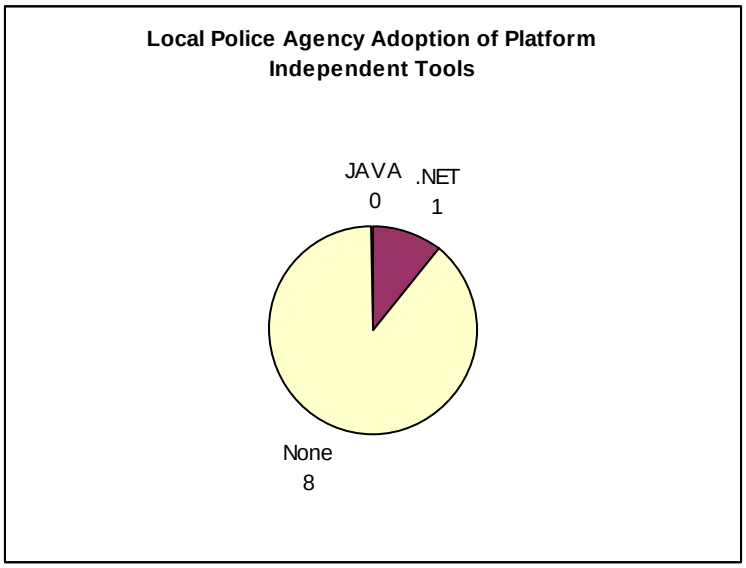
Of the COTS solutions used by respondents, Sleuth was clearly the most common product deployed in the local police departments.



The variety of DBMS used for persistent storage in the RMS (including the custom-built applications) was fairly spread, with the category of "Other" having the largest share at 40%; however, the DBMS in use in these deployments was not identified. It appears the Sleuth product may have its own proprietary database, though some Sheriff Offices with the same solution indicated it was a SQLServer solution.



The use of platform-independent tools that could be used to facilitate integration of the RMS systems with police agency information exchange partners has not yet been firmly established. When asked about the use of .NET or Java implementations, the majority of those responding indicated they had no such deployments in their current IT environment.

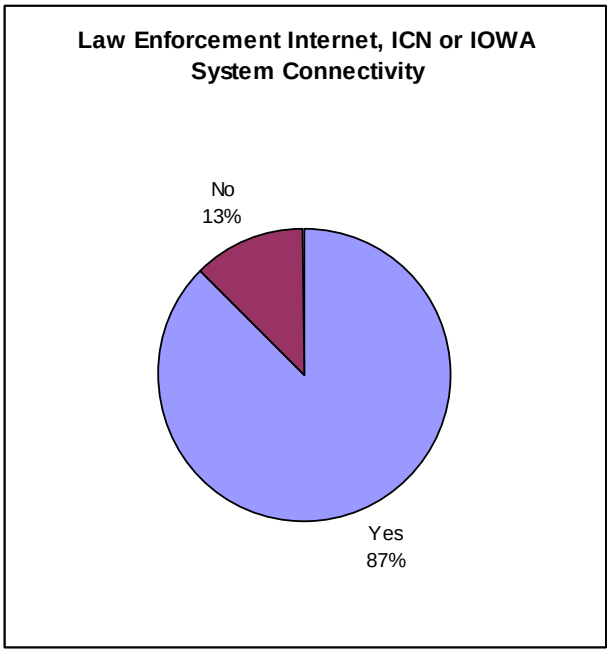


No major trends in the areas of enhancements to the technical environments were apparent from the responses received from the local law enforcement agencies, though

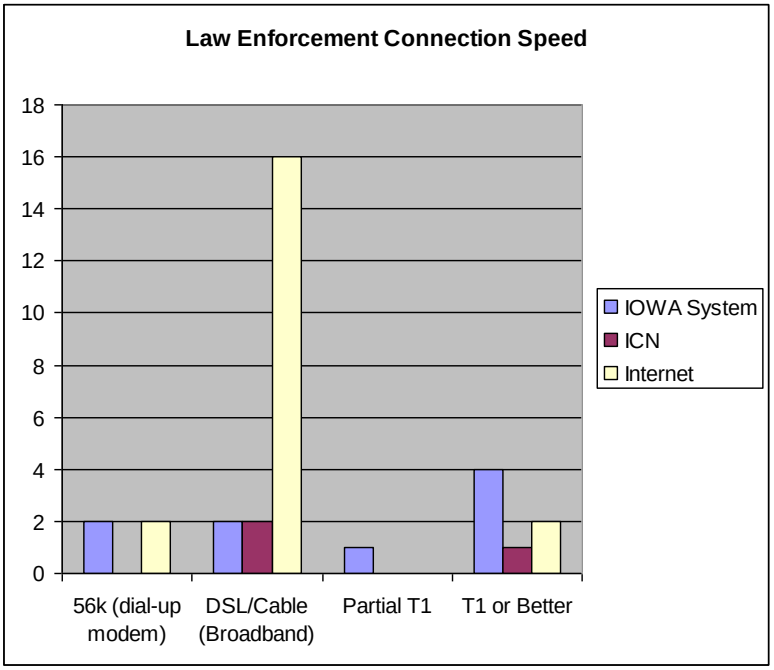
there were some minor shared areas of interest. Examples include efforts to deploy Mobile Data Terminals (MDT) and projects sharing CAD/RMS resources with the other law enforcement agencies and/or the county Sheriff's Office.

3.4.13.2 Network Connectivity

A solid majority of the responding police departments have access to one or more broad network infrastructures in Iowa. When asked if their agency maintained access to ICN, the IOWA System, or the Internet, 87% stated "Yes."

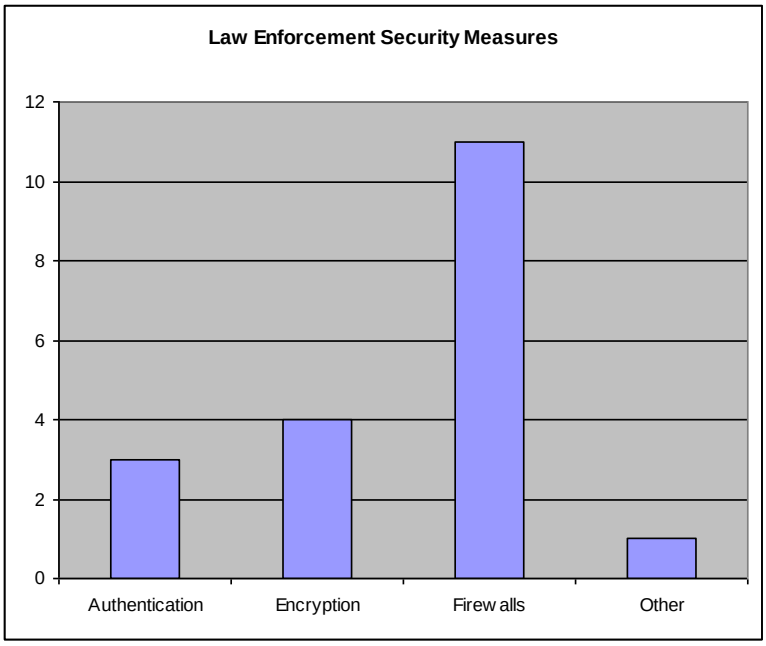


Those responding "Yes" to having connection to one or more of the identified networks were also asked to provide the connection speed they maintain to the various infrastructures. The connections ranged from 56k dial up to T1 capabilities. The vast majority of respondents maintained a connection to the Internet with broadband speed (DSL or Cable). The following bar graph indicates all of the connection speeds maintained for the three communication networks inquired about:



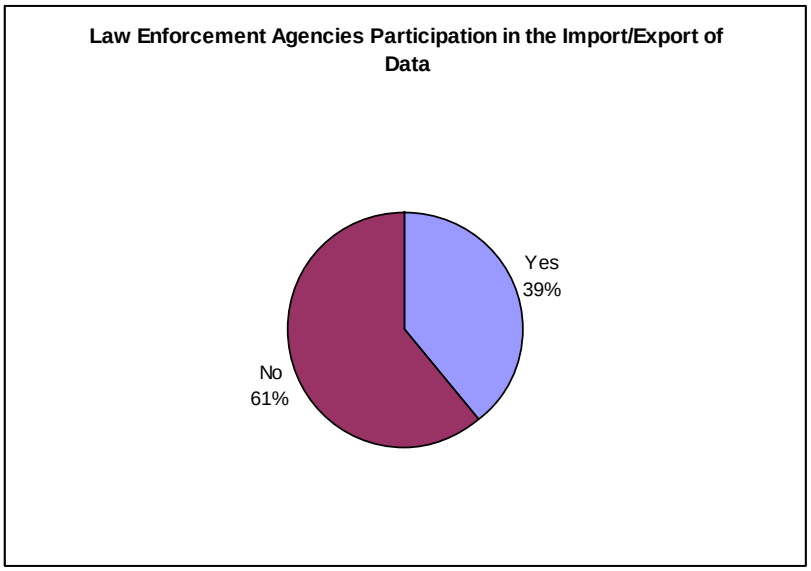
3.4.13.3 Current Security Policies

The local police agencies were also asked about the use of security measures in their applications and network infrastructure. Each was asked if they utilized authentication, encryption, firewalls, or any other method to help secure their data and network traffic. The following bar graph depicts the responses received from the local law enforcement agencies.

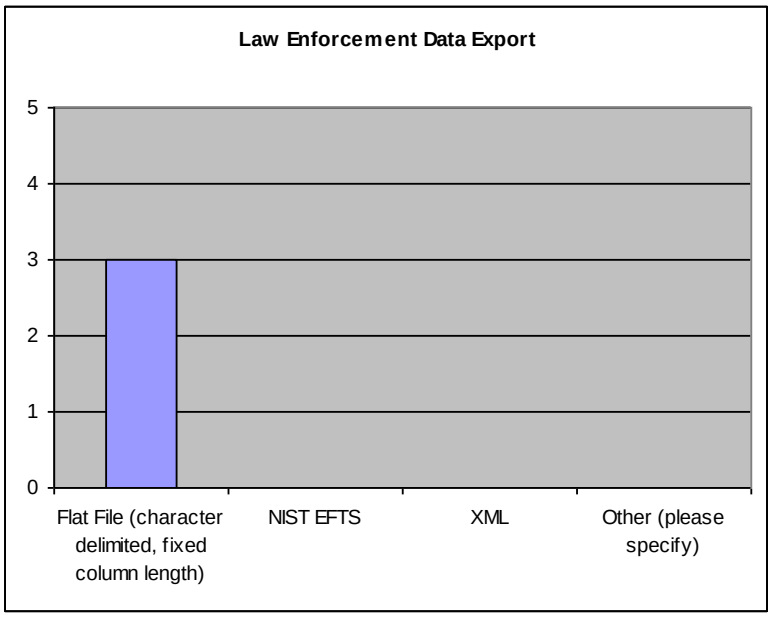


3.4.13.4 Data Standards

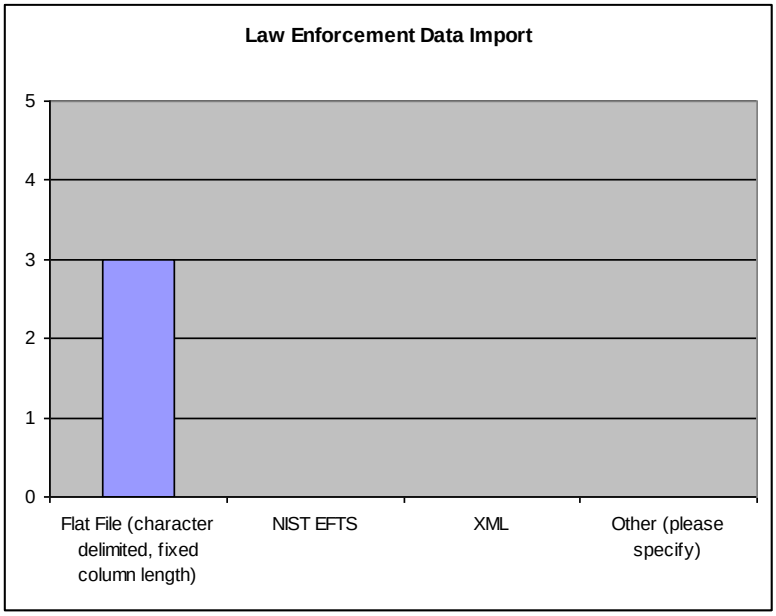
Iowa Police Departments responding to the survey do not have a large amount of information sharing between other systems currently taking place. When asked if their agency currently imported or exported data between internal or external systems, 39% responded "Yes."



Details about how the agencies that are exporting data are structuring the data lead to the discovery of a universal use of flat files (either character delimited or fixed column length). The use of metadata standards such as XML or NIST EFTS was yet to be adopted for exporting data. Over half the agencies (57%) exporting data indicated that they did have a documented formal policy for how information can be shared.



The same conclusion held true (based on our low response rate) when police agencies were asked how data was structured when imported to their systems. Again, flat file structured data was the only format selected by agencies who responded that they import data into their applications.

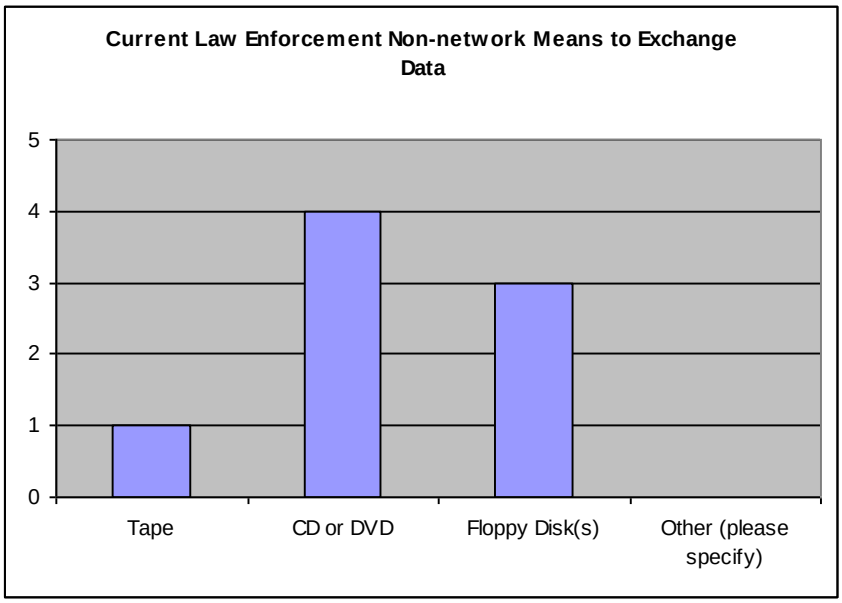


3.4.13.5 Transaction Processing Capability

An event-driven model for sharing information using a guaranteed messaging architecture does not yet exist in the Iowa police departments responding to the survey.

When asked if they used MQ Series, Java Messaging Service, WS-Reliability, or some other guaranteed messaging protocol, no selection was made.

When asked about their use of non-network methods for sharing data, local law enforcement agencies identified a variety of media used to transfer data into and out of their applications. The following bar graph displays the use of tape, CD, floppy disk, and other medium used by the responding agencies for sharing their data.



3.4.13.6 Adoption of Web Service/SOA Standards

The adoption of web services and SOA architectures is an area of technology where the local law enforcement agencies are not rushing to implement. Participants were asked if they were using, or had plans to use in the next 18 months, web services, UDDI, SOAP, or XML schema. Only two respondents indicated that they were using or had plans to use web services in the time period indicated.

3.4.14 Enterprise View

3.4.14.1 Current Systems Environment

The Judicial Branch, as represented by the SCA, DOC, DPS, DOT, and CJJP, together represent the most significant portion of the foundation for an integrated Justice environment in the State of Iowa. Each of those participants currently maintain at least one major information system to handle their internal business processes as well as administer multiple interfaces between themselves and local law enforcement agencies. They are already exchanging data on a daily basis, and in some cases, a real-time basis. While some legacy technology systems exist within DOT and DPS, each has systems that

are already either web-enabled or web-based utilizing current RDBMS products for the database layers.

3.4.14.2 Network Connectivity

Any statewide, integrated justice effort requires that all local and State participants be interconnected. Fortunately, the ICN fiber WAN has a point-of-presence in each county, private telecommunications companies provide local feeds to the ICN, and each of the above mentioned participants have established use of the ICN for their systems. The ICN is a separate entity, and as such, provides and administers the network usage in cooperation with the SCA, DOC, DPS, DOT, and CJJP via service level agreements. In the case of DOC, a private software vendor, ATG, manages the Department's use of the ICN on their behalf. DPS has the most restrictive network requirements due to its adherence to established NCIC protocols for secured access. However, the means to connect all CJIS participants statewide exists via the ICN and is already in use by these major State participants and their systems.

3.4.14.3 Current Security Policies

Justice data by its nature requires a secure environment for information system processing, and these major systems all take this into account by providing secure transmission, user training, and user account management and level of access controls based upon job function. Additionally, these systems all implement their own level of control with respect to network access by either directly or through ICN staff, configuring firewall controls and access control lists. IOWA System users must also adhere to NCIC certification and audit criteria, its Rules and Regulations, as well as user, location, and terminal identification. A paradigm of security protocols and practices is already established, and any effort to move existing interfaces to transaction-driven data exchanges within the context of a workflow must not detract from existing practices. However, streamlining the data exchanges between these large systems affords the opportunity to apply best practices more uniformly across the enterprise.

3.4.14.4 Data Standards

The majority of data exchanges occur as FTP-based flat file transfers in batch with file layouts being specific to the needs of each particular interface. Exceptions to this include protective order transactions restructured as message switch transactions, pre-sentence investigation interfaces using SQL against an intermediate staging database, parole and probation inquiries of ICON via Kaleidoscope, real-time driver's license, vehicle registration, and reciprocity inquiries utilizing XML as well as Livescan/AFIS transactions. What is lacking is a common denominating data standard for these exchanges. The use of XML is not a foreign concept to any of these major State participants, and all have, in some form or another, approached the use of it in updating their existing interfaces. However, the efforts have been isolated from each other and usually utilize a markup scheme specific to the particular systems involved. To move forward with an integrated justice effort, a common, XML-based data standard will need to be the norm rather than the progressive exception, inclusive of the GJXDM standard

model. These major participants can technically do this already to some extent. What remains is to coordinate an analysis of these exchanges so that a common denominating data standard germane to all can be utilized.

3.4.14.5 Transaction Processing Capability

Transaction-based data exchanges are the exception rather than the rule in these major participants' current systems interfaces. However, the exceptions to that trend demonstrate significant promise with regard to cross-agency justice information sharing in Iowa. This is especially evident with the DPS exchanges with the DOT Driver's License, Vehicle Registration, and Reciprocity systems as well as the Livescan/AFIS processing. It is also in place to an extent with protective order entry. Additionally, TraCS provides a solid example of the adoption of a streamlined workflow to drive the process of safety data collection far more efficiently than before. A serious effort in analysis, design, and development will be necessary to not only identify the necessary event triggers to drive transaction-based processing but to, in general, elevate all of these systems' interfaces from the current batch-mode processing to real-time, event-driven transactions. Inroads have already been made from the examples given, and from a technical perspective, while effort will be involved, this is a logical enhancement and extension to a technical direction already being set forth.

3.4.14.6 Adoption of Web Service/SOA Standards

Service-oriented architectures are not currently the norm for these major State systems as most data exchanges are done as scheduled batches. Additionally, some existing transaction-based exchanges such as Livescan/AFIS and Protective Order entry, while they occur real-time, represent a more specific implementation of data transfer methodologies rather than the consistent use of a service-oriented architecture. Existing data exchanges between DPS and the DOT Vehicle Registration and Reciprocity systems are already web service-based and represent an established implementation. From a technical viewpoint, moving towards a service-oriented architecture is not so much a question of why or when for these major participants, but rather how it is best implemented. With the Open FOX message switch moving towards handling web-services this year, a significant piece of existing data exchanges (as they apply to DPS systems) can be moved into the service-oriented architecture model. The technical skills are already able to be leveraged by these participants; however, the design, analysis, and development effort necessary to enhance these existing systems and their existing interfaces will be serious.

3.4.14.7 Summary

In summary, the information systems employed by the State Court Administrator's office, the Department of Corrections, the Department of Public Safety, the Department of Transportation, and the Criminal Juvenile Justice Planning division are already exchanging data. They are already aware of the current limitations of these interfaces in that they grasp the design and nature of the transaction-based and workflow-driven architecture of an enterprise-wide integrated justice implementation. Updates to existing

systems in terms of utilizing service-oriented architectures and transaction-based processing will be necessary and do not represent a trivial amount of work or coordination. Additionally, the inroads established in the use of XML need to be expanded to utilize a common XML-based data standard across the enterprise. Again, this will be a significant effort in analyzing existing interface formats and moving them to a general data standard such as the GJXDM model. However, for these major participants, these efforts are natural extensions and enhancements of the existing vision for the future of these systems.

4 To-Be Iowa CJIS Description

4.1 To-Be Business Environment

The To-Be Business Environment section will outline the recommended new/modified business processes necessary to successfully implement CJIS, their identifiable risks to success, as well as how they will help facilitate integration standards required for the Iowa CJIS solution.

4.1.1 To-Be Business Process Environment

The To-Be Business Process Environment section will provide the detail of what business initiatives, agreements, practices and processes will need to be established if the CJIS initiative is to be achieved in Iowa. Much of the section will address how to fill the gaps that currently exist, which are barriers to integration. These gaps were originally identified in the As-Is Business Assessment.

4.1.1.1 General Concepts for the Justice Enterprise in Iowa

The State of Iowa has made great strides over the past several years in planning for and implementing cross-agency criminal justice information sharing. An active governance structure has been established and the State has undertaken several studies that recommend strategies for integration. In addition, agencies and the Judicial Branch have come together to automate key exchanges, such as the real-time passing of the protection order from the Judicial Branch to the Department of Public Safety (DPS).

However, to move to a fully integrated statewide approach to criminal justice information sharing, several enterprise-wide issues will need to be addressed. As has been well documented, among the State's 99 counties there are significant variations in business practices and forms used in the exchange of information. This results in disparities in the manner in which information is collected and shared, thus making the ability to electronically share the information far more difficult. In addition, there is currently no framework available to all agencies by which information can be exchanged in any coordinated way; each automated exchange that has been implemented has been negotiated specifically between the affected agencies.

To overcome these challenges, the MAXIMUS/URL Team proposes a strategy that includes the following components:

- The creation of an empowered governance, organizational, and project management structure that promotes the oversight and management necessary to move from CJIS planning to implementation;

- Adopt SOA to allow for an integration framework based upon industry open standards (WS-I), which will still maintain system autonomy through the exposure of loosely coupled services;
- A centralized CJIS integration or messaging Broker[27] and business process manager to facilitate the exchange of information between agencies that is mindful of disparate security policies and uses the commonly accepted GJXDM-conformant schemas;
- The incorporation of key identifiers into workflow documents to provide for the ability to track a person, incident, or case throughout the justice process;
- The development of a standard Iowa justice domain model, through the creation of a statewide common GJXDM subset and extension data model and dictionary for information that is shared between the participating systems and necessary for automated processing to occur;
- Build off of the successes that Iowa has previously demonstrated in automating exchanges, such as the protection order exchange, and the PSI exchange;
- The use and expansion of the Department of Transportation's TraCS in an SOA environment as a manner in which electronic filing with the Courts can occur, both for law enforcement and County Attorneys;
- The promotion of standardized business practices and forms among practitioners; and
- Leverage concurrent automation activities, such as the common charge table that the County Attorneys are preparing for their Case Management initiative.

The vision of the strategic criminal justice enterprise must include proactive steps for transition from a world in which automation is largely nonexistent or happens on a nightly basis through batch FTP exchanges to one where information is exchanged on a real-time basis, as a part of day-to-day workflow activities. From a business process perspective, this will require a shift in thinking about workflow and consensus on how to direct the technical modifications to both maintain and improve the business operations of the agency as a result of the automation.

[27] This CJIS Broker manages the messaging non-functional requirements (i.e., gets information where it needs to be when it needs to be), is secure and from an authenticated source and manages business flow based on rules and content of messages. Agencies simply need to know what they want to accomplish from a business perspective and what rules the Broker will enforce to move the message (exchange) along. This will result in the sharing of the right information at the right time and will improve the quality and integrity of information within the enterprise.

4.1.2 Business Recommendations

4.1.2.1 Governance/Project Management

4.1.2.1.1 Create an Expanded Governance Structure for CJIS in Iowa

In order to implement CJIS in Iowa, there will need to be changes made to the governance model and the statutory authority for oversight of CJIS implementation in Iowa.

Options

1. Amend the existing Memorandum of Understanding to expand the role of the CJIS Advisory Committee to include the following:
   - Expand the CJIS Advisory Committee to include a representative from the Department of Transportation;
   - Recognize the role of the Planning Committee as the organization that provides direction for the CJIS implementation effort and project management team; and
   - Provide ongoing direction for the management and necessary resources for CJIS implementation in Iowa;
   - Create and recognize the CJIS Program Office (see Sections 4.1.2.1.2 and 4.1.2.1.3 below) and allocate appropriate authority consistent with those recommendations; and
   - Address issues around legal ownership of data and information included in the CJIS solution.
2. Maintain the existing governance documents with no changes.

Recommendations

The MAXIMUS/URL recommendation is to adopt Option #1 above, to expand the existing CJIS charter, and direction to address implementation-focused activities.

Benefits

A clear charter and expectations around governance and strategic direction is critical to ensuring the success of the CJIS implementation effort.

4.1.2.1.2 CJIS Organizational Issues

The architecture proposed by the MAXIMUS/URL Team will need to be managed and administered. As such, issues around where the CJIS Broker is maintained and who is responsible for supporting and staffing the overall CJIS initiative is an important consideration.

Options

There are several options associated with this issue:

1. The CJIS Broker could be housed in an existing state criminal justice agency such as Public Safety, Corrections, or the Courts.
2. The CJIS Broker could be its own independent, stand-alone agency.
3. The CJIS Broker could be housed in the Division of Criminal and Juvenile Justice Planning (CJJP).
4. The CJIS Broker could be housed in the Information Technology Enterprise (ITE) within the Department of Administrative Services.
5. The CJIS Broker could be coordinated jointly by the Division of Criminal and Juvenile Justice Planning and the Information Technology Enterprise via inter-agency agreements.

Recommendation
We recommend that the CJIS Broker could be coordinated jointly by the Division of Criminal and Juvenile Justice Planning and the Information Technology Enterprise via interagency agreements, in a CJIS Program Office located within CJJP. We envision CJJP acting as the body that directs and manages all program, business-related, and technical policies and activities, under the direction of the CJIS Advisory Committee and CJIS Board. We envision ITE supporting the CJIS effort technically, as directed by the CJIS Program Office, by hosting the CJIS Broker and providing programming support and other maintenance-related activities.

Because ITE provides broad technical support to Executive Branch agencies and procures its own rules, standards, and procedures regarding information technology in Iowa, the interagency agreement that supports the relationship between CJJP and ITE would need to include provisions that ensure that the direction set forth by the CJJP can be fully implemented by ITE. In some instances, the CJIS effort may need to request an exemption from the newly created CIO Council from specific standards if deemed in the best interest of the CJIS effort by the Board and Advisory Committee.

Benefit
The benefit of this approach is that it would maximize the existing expertise within each agency. CJJP possesses the business knowledge of the justice community, and ITE possesses the technical skills. This would maximize existing staff and other resources thereby saving money. This arrangement would also be consistent with the missions of both agencies.

4.1.2.1.3 CJIS Funding Issues

Funding to support CJIS implementation is crucial to its success. The activities around soliciting funds are multi-faceted and can include both fundraising and budget preparation and review activities.

Options

1. Allow the CJIS Program Office to continue soliciting grant funds to support CJIS implementation activities;
2. Create budgeting authority in the CJIS Program Office to create a yearly CJIS budget for presentation to the legislature;
3. Allow for the conditioning of new grant funds for projects and initiatives that are consistent with the statewide CJIS Plan;
4. Encourage the development of new justice technology activities be coordinated with the CJIS Plan.

Recommendation

The MAXIMUS/URL Team recommends all four options above: to expand the role of the CJIS Program Office to not only seek funds but help ensure that new initiatives that are supported with state or federal funds develop in lockstep with the statewide CJIS Plan.

Benefit

While a resource intensive activity, the creation of a CJIS Program Office and its authority to raise and monitor funding around justice technology is an effective way to ensure that the CJIS effort is well funded and all other justice technology efforts are developed consistent with the CJIS strategic vision.

4.1.2.1.4 Project Management

The implementation of the CJIS strategic plan and the activities around business process change, forms consolidation, and schema development will require a significant project management effort.

Options

1. Empower current CJIS Project Manager within CJJP with authority to conduct project management activities, including hiring staff and/or contractors to complete the work.
2. Leverage staff from existing agencies to lead CJIS project management activities in addition to their own responsibilities.

Recommendation

Empower current CJIS Project Manager by creating a CJIS Program Office within CJJP with authority to conduct project management activities, including hiring staff and/or contractors to complete the work. Implementing this approach will require an investment of resources with regard to staffing and planning assistance.

Benefit

Having individuals whose sole role is to manage the CJIS integration implementation effort is critical to ensuring its success. While it is beneficial to have feedback from and

participation from other agencies, managing CJIS implementation is more than a full-time effort.

4.1.2.1.5 Outreach to Local Justice Practitioners

The MAXIMUS/URL survey results indicated that many local level justice practitioners had significant concerns about the CJIS effort. Responses expressed trepidation regarding the effects of the initiative on already taxed staff. In addition, there were concerns about unfunded mandates and the costs associated with procuring new equipment, software, and the like.

Ironically, the goals of the CJIS effort in Iowa are to improve staff efficiencies by reducing redundant data entry and improving the quality of information with which practitioners do their jobs. Another objective is to leverage existing systems and maximize the use of technologies such as XML that can provide a communication mechanism between disparate systems.

Options

1. Create a multi-faceted communications strategy that leverages the CJIS Advisory Committee, professional associations, and other methods to disseminate information from practitioners regarding the statewide CJIS effort in Iowa.
2. Conduct outreach activities (posting items to websites, sending out e-mails) on an ad hoc basis.
3. Rely solely on CJIS Advisory Committee members to communicate to their constituents about the progress of the CJIS initiative.

Recommendation

The MAXIMUS/URL Team recommends that the CJIS Project Manager draft a multi-faceted communications strategy that leverages the CJIS Advisory Committee and professional associations to disseminate information from practitioners regarding the statewide CJIS effort in Iowa. This recommendation is consistent with the requirement in the Memorandum of Understanding between the Executive and Judicial Branches to develop a communications plan to build consensus among the members of the criminal justice community and secure state and local support for the CJIS initiative.

Benefit

Taking a planned, multi-faceted approach to outreach will help ensure that information about the CJIS initiative is distributed to all target audiences and that the message delivered is consistent among groups. This effort will help ensure that all local level justice technology activity in the future is coordinated and has goals that are consistent with and contribute to statewide integration.

4.1.2.2 General Workflow Recommendations

4.1.2.2.1 Encourage Real-Time Data Entry

The automated exchanges that are currently occurring in Iowa, with the exception of the protection order, are conducted via batch FTP transaction rather than real-time information sharing. As such, these exchanges are not incorporated as part of the everyday workflow within affected agencies. The long-term goal of the strategic plan should be to encourage real-time information sharing that is part of the overall business process.

Options

1. Keep writing custom exchanges between agencies
2. Implement a service-oriented architecture (SOA) to facilitate information sharing

Recommendations

Implement SOA to facilitate information sharing.

Benefit

The SOA approach is discussed in greater detail in the Technical To-Be section below, but from a business perspective, a SOA will afford the transition to a real-time, workflow dependent information exchange by providing the exchange functionality with as little impact as possible upon the current application solutions being utilized for support of the participating agencies business processes.

4.1.2.2.2 Resolve Disparate Forms and Business Practices

The previous exchange analysis studies, as well as the As-Is Assessment conducted by the MAXIMUS/URL Team, indicate that the disparity in business process and forms MUST be rectified before automation can take place. With previous pilot projects and exchanges, there have been several successful efforts in Iowa to bring people together to standardize on forms, documents, and practices.

Options

1. Have a single agency identify changes to forms and mandate changes statewide
2. Create working groups to come together to discuss changes to the business process, contents of common forms, etc.

Recommendations

Specific examples of exchanges this should affect are listed below. Specific recommendations include:

- Create working groups to assist in the business process change; focus working group efforts to standardize on forms and business practice on first phase exchanges, as identified in URL's Adult Exchange Analysis study.
- Engage justice professional associations to assist in sponsoring standardization working group efforts, communicating efforts to constituents.
- Use GJXDM-conformant schemas as the vehicle to describe information between disparate systems.

Benefits

- Bringing people together to discuss changes to business processes will help ensure that the changes are implemented in practice.
- Involving professional associations will help with outreach.
- SOA using GJXDM-conformant schemas is a well thought out and vetted data model for sharing information in the justice domain.

4.1.2.2.3 Disparate Security Requirements

The As-Is Assessment completed by the MAXIMUS/URL Team indicated that the security requirements – especially among large State systems – differ significantly. Agencies that intend to interface with the DPS need to either adapt to the DPS security standards or construct interfaces – such as the protection order interface.

Options

1. All agencies adopt DPS security requirements (NCIC certification and IOWA System Rules and Regulations compliant).
2. Exchanges with DPS should leverage the process used to create the protection order interface.
3. DPS does not participate in automated information exchange with other agencies.

Recommendation

The MAXIMUS/URL Integration Team recommends that exchanges with DPS should leverage the process used to create the protection order interface. This will require continued work and partnership between DPS and the NCIC auditors, to ensure that integration in Iowa can move forward while maintaining compliance with NCIC certification rules.

Benefit

There are important lessons learned from the experience and while the protection order exchange was intricate and cumbersome to implement, it allows real-time transactions between Courts and DPS without Judicial Branch personnel being subject to the NCIC certification and IOWA System Rules and Regulations.

4.1.2.2.4 Digital Representation of Authenticated Signature in ICIS

Currently, TraCS does not perform electronic filing (e-filing) with the Courts because of the inability of ICIS to capture the digital signatures from the TraCS system. Rather, there is an exchange between TraCS and ICIS at present on traffic violations with appearances. The information is initially passed via FTP to a file server at DPS from where it is retrieved by ICIS. TraCS captures the signature image of both the officer and the defendant but this is not a part of the information exchanged.

The Iowa Constitution requires that any criminal filing include both the signature of the officer as well as a notary signature. In addition, non-scheduled criminal offenses require the notary to present a stamp or seal verifying the notarized signature.

While TraCS citation information populates ICIS, the Court still currently requires the paper citation as the official filing document, since the condition of the filing is the notarized signature.

The notary signature issue is only applicable in criminal cases; the Iowa Judicial Branch is planning to implement e-filing in the Civil Court process in 2006, beginning with pilot projects. The Judicial Branch intends to use commonly accepted court filing standards (OASIS, XML) with this effort.

Options

1. Provide Court rule or statute change to allow digital representation of authenticated signatures in ICIS to accept e-filing.
2. Modify ICIS to accept digital signatures, employing Public Key Infrastructure (PKI) security technologies to support the authentication of verified signatures necessary for criminal e-filing.
3. Conduct business process review and change involved in accepting digital signatures and ensuring compliance with the Atsinger decision and the need for independent verification of criminal complaints.
4. Encourage all electronic court filing processes to use open architecture standards.
5. Request legislative modification to allow for an electronic certification to replace the stamp/seal requirement for the notary required for nonscheduled offenses.

Recommendations

We recommend undertaking all of the options above to facilitate the ability to pass digital representation of signature along with document to allow for e-filing and electronic orders. PKI technologies ensure that legitimacy of a sent and received message by employing a pair of mathematically related cryptographic keys. If one key is used to encrypt information, then only the related key can decrypt that information. If you only know one of the keys, you cannot easily calculate what the other one is. This will help ensure that the filing is not accepted until both pieces of information (officer signature and notary signature) have been executed.

Benefits

This will help facilitate electronic information sharing between TraCS and ICIS and create an e-filing solution for appropriate criminal cases in Iowa that comports with the Judicial Branch's overall vision for electronic case filing.

4.1.2.3 Disparate Levels of Automation

In order for all justice agencies to participate in the statewide CJIS effort, there will need to be a concerted effort to ensure access to automation among all agencies. From our As-Is analysis, we have learned that there is an issue surrounding lack of automation for some County Attorney and Law Enforcement agencies in Iowa. It is also clear to us that there are efforts underway, such as the County Attorney Case Management Project that mitigate the effects of this situation. In addition, the Department of Transportation's TraCS system is in use in a number of local law enforcement agencies and could be leveraged as a manner for these smaller agencies, without Records Management Systems (RMS) to participate in the statewide integration effort.

What must be better understood is the status of technology in these agencies, especially among local law enforcement agencies. In addition, the existing capacity of larger agencies that have their own CMS or RMS systems and their ability and willingness to modify those systems with interfaces that become the common standard for charging and electronic filing must be assessed.

4.1.2.3.1 Leverage TraCS for Future Law Enforcement Agency Development

When distributing the MAXIMUS/URL survey, the CJIS Project Manager and DPS reported concerns that there were only e-mail addresses for approximately half of the State's law enforcement agencies, and that a significant number of local law enforcement agencies would not have the opportunity to respond. Furthermore, it is unclear how many local law enforcement organizations use information systems such as Records Management Systems (RMS) and/or Computer Aided Dispatch.

From our interview with Department of Transportation (DOT) officials regarding the TraCS effort, many small local law enforcement agencies use the TraCS as an ad hoc RMS. TraCS currently supports important law enforcement agency (LEA) documents such as Complaints and Incident Reports. These documents should also move to an SOA environment when exchanging with justice agencies and should be leveraged in both the standardization of these documents statewide as well as the proposed technical architecture.

Options

1. All Law Enforcement Agencies must use TraCS for all of their law enforcement transactions.
2. TraCS should support all law enforcement agency e-filings, Citations and Complaints, and Incident Reports as well as support the use of agencies' RMS for these documents. It should do so by providing XML exchanges between TraCS and the RMS as well as the capability for the RMS to use the XML schemas to produce conformant Complaints and Incident Reports, so as to be flexible enough to allow local agency preference.

Recommendations
TraCS should support all law enforcement agency e-filings, Citations and Complaints, and Incident Reports as well as support the use of agencies' RMS for these documents. The MAXIMUS/URL Team believes that this recommendations broadens the ability of smaller agencies to participate in the integrated justice solution while not precluding larger agencies with robust RMS in using those systems to conduct their everyday business processes and future automated exchanges with other agencies.

Benefits
This is discussed in further detail below, but we recommend that TraCS have the capability of exchanging standardized forms (Complaints, Citations, Incident Reports) based upon GJXDM-conformant schemas, which we encourage to be designed identical to those generated from law enforcement agencies and Sheriff Offices using their own RMS. In other words, the MAXIMUS/URL Team believes that an expanded TraCS should have the ability to support all of the charging documents directly and through XML populate the RMS if the local agency so chooses.

4.1.2.3.2 Support of County Attorney CMS Project

Lack of automation appears to be a problem for the County Attorneys in particular. The previous URL studies noted that prosecutor charging behavior should follow more a predictable pattern and that a common case management system should be supported. Currently, the County Attorneys Association in Iowa is supporting a pilot automation effort with funding from CJJP to provide one of two Case Management Systems (CMS) to prosecutors. Thirteen counties have begun using the CMS by summer of 2005.

Options
1. CJJP continues support of this effort after the initial pilot.
2. CJJP continues support of this effort after the initial pilot and encourages County Attorneys to continue developing the project with the statewide strategic plan in mind.

Recommendation
Our recommendation is that CJJP continues support of this effort after the initial pilot but also encourages the County Attorneys to move forward in lockstep with the statewide strategic plan and its recommendations for SOA compatibility, GJXDM conformance, and standardized business processes. Any financial assistance provided should place a contingency on the evolution of the County Attorneys' software, business practices, etc., and requires that it be in sync with the statewide CJIS strategic plan.

Benefit
A common case management system among County Attorneys will greatly assist in integrating the justice system in Iowa. It will make the automation of important exchanges, such as the law enforcement charging process and the exchange of delinquency petitions to the Court much easier.

4.1.2.3.3 Utilize Persistent TraCS data for County Attorney Filing Decisions

If TraCS is to be the standard or share the standard for LEA charging documents and the Incident Report, the County Attorneys will have the ability to consume these exchanges documents once they have a system to do so. As TraCS documents will be persistent, this could be a mechanism for County Attorneys to view the charging document (via a web page), act upon it, and submit it to the Court or whatever routing is appropriate. The document would be supported with a style sheet.

As the CMSs come online or gain the SOA capability, the documents would be managed through the CMS as opposed to the above described mechanism.

Options

1. Prosecutors should have query access to charges initiated by LEA/Sheriff's Office in the TraCS central repository in instances in which they have their own CMS.
2. Prosecutors without a CMS should have the capability to view information in TraCS and make charging decisions based upon the charges in the TraCS.

Recommendations

The MAXIMUS/URL Team recommends both options to allow for County Attorney participation in an automated charging process, notwithstanding what their current state of automation/CMS use is in the jurisdiction.

Benefits

All County Attorneys would be able to participate in the CJIS solution under one of the two recommended structures.

4.1.2.4 Standards

4.1.2.4.1 Move Existing TraCS Electronic Citation Component (ECCO) to SOA

Moving TraCS from a file-based process to a transaction-based process will provide a more reliable ECCO data integration solution and will allow for e-filing to occur in Iowa in a consistent manner.

Options

1. Exchange the Uniform Traffic Citation through a GJXDM-conformant schema for the Court and a persistent TraCS repository.
2. Continue with TraCS as a decentralized, file-based system.

Recommendations

Exchange the Uniform Traffic Citation through a GJXDM-conformant schema for the Court and a persistent TraCS repository. This recommendation was also made in the CISCO report. The MAXIMUS/URL Team also suggests that this recommendation apply to all future TraCS documents.

Benefits
This modification will make TraCS robust enough to act as a key repository for exchange of filing information with the Courts.

4.1.2.4.2 Standardize All Court Filing upon Developing Standards

A movement toward e-filing, as promoted in the above recommendations, should be consistent with emerging standards.

Options
1. Research and adopt appropriate Court e-filing standards, such as those promulgated by OASIS.
2. Develop separate filing processes, information exchange schemas, and standards based on unique case type.

Recommendations
The MAXIMUS/URL Team recommends Option #1 above. The Courts should not have to respond to filings in a variety of architectures based upon case type. There are Court e-filing standards for SOA in the final stages of development that should be leveraged in Iowa. This type of filing would include e-Citation, prosecutor, and civil filings. The filings could occur across a closed network or the Internet.

TraCS filings should take into consideration these standards as well as filings developed from County Attorney CMS such as Judicial Dialogue. The County Attorneys should also be able to file a Trial Information via a secure web site. The standards define the non-functional requirements that ensure security and authentication across the Internet. Filings with the Court could simultaneously meet the current function of the Greensheet and update the CCH with prosecutor dispositions again through a secure environment.

Benefits
Leveraging the OASIS standards would provide two immediate benefits to the CJIS effort in Iowa: 1) leveraging the OASIS work provides a quick and easy infrastructure for e-filing in Iowa and 2) conducting e-filing in a uniform fashion for all cases would simplify the filing process for the Court Clerks and other Court personnel.

4.1.2.5 Common Forms and Practices

4.1.2.5.1 Standardize and Expand Law Enforcement Forms

There is a need for standardization among important law enforcement reports, such as Citation, Complaints, and other charging documents. TraCS currently contains many of these forms, which have been standardized among local law enforcement agencies using TraCS.

Options

1. Leverage the planned TraCS OWI Complaint form for reusability across other non-traffic offenses requiring a Complaint (could include simple misdemeanors).
2. National Incident Based Reporting System (NIBRS)-compliant Incident Report TraCS has developed should be considered for statewide use across offense types.

Recommendations
The MAXIMUS/URL Team recommends both options be undertaken and that generally, TraCS forms are leveraged for broader use. Any changes or expansion to these forms should include input from LEAs, Sheriffs, and County Attorneys.

Benefits
Leveraging existing infrastructure with a system as pervasive as TraCS will help ensure that many agencies are able to participate in the integrated justice solution. In addition, emerging Incident Report standards including N-DEX and Global Information Exchange Package Definition (GIEPD)[28] may be helpful in providing assistance in standardizing the Incident Report across offense types.

4.1.2.5.2 Standardized LEA Non-Traffic Charging Documents and Incident Report Must Be Available Outside of TraCS

As suggested in Recommendation 4.1.2.3.1 above, the MAXIMUS/URL Team believes that TraCS is a system to be expanded and leveraged by the Courts and ICIS for electronic filing. However, we know that larger law enforcement agencies may not intend to use TraCS as their primary system of record and rely on their own RMS systems to create important documents, such as charging documents and Incident Reports.

Options
1. Create important forms and documents – for both TraCS and other RMSs – using standardized GJXDM schemas, enumerations, and style sheets.
2. Create a TraCS schema and separate custom schema for all agencies that intend to use their RMS to create these important law enforcement forms and documents.

Recommendations
The MAXIMUS/URL Team recommends Option #1 above, the creation of these important documents for both scenarios using GJXDM-compliant schemas. These agencies should have the option to incorporate the non-traffic charging documents into their RMS by making available the standardized schemas, enumerations, style sheets, and other artifacts to the LEA or their designated vendor.

[28] GIEPD are contextual-based conceptual models, schemas and associated documentation to provide a reference for identified business documents using the GJXDM. More information is available on the OJP website at www.it.ojp.usdoj.gov.

As recommended above, TraCS will have the capability of exchanging standardized Complaint forms based upon GJXDM elements identical to the ones being generated from law enforcement agencies and Sheriff Offices using their own RMSs.

Benefits
This recommendation is broad enough to allow local law enforcement agency preference in participating in the CJIS solution depending on their current level of automation.

4.1.2.5.3 Standardize Exchange of Charging Documents

Currently, charging behavior varies among jurisdictions. In some areas and dependent on the type of case, charging decisions are filed by County Attorneys but in some cases also by law enforcement.

Options
1. Continue the disparate business practice.
2. Create a rule-based exchange for charging documents.

Recommendations
The MAXIMUS/URL Team recommends Option #2 above. TraCS is currently the vehicle for electronically exchanging traffic Citations scheduled for Court appearance to ICIS. If TraCS is expanded (consistent with our recommendations above) to have a broader role in exchanging Complaints with the Courts and also County Attorneys, standardizing this process is very feasible, as the County Attorney would have the ability to review the Complaint prior to the Court receiving the document. LEAs will require a case-by-case option for routing as well as the ability to establish rules (both local and state).

Benefits
This option would both standardize the charging process, which would likely make receiving the charges easier for the Court Clerks.

4.1.2.6 Traceability

The ability to trace relationships between incidents, cases, and people is integral to an automated workflow process in the criminal justice enterprise. Law enforcement may view a "case" based upon an incident or series of incidents being investigated. Charges may be brought against a suspect in that case, which may or may not result in an arrest. The County Attorney may choose to file a case based upon the charges originally brought by law enforcement or may change the charges and file new or different charges with the Court. The Court opens a case based upon a filing and disposes the case. All of this can occur without a positive identification number or DCI#, or all of this can occur without a Document Tracking Number (DTN), but none of this will occur without each agency having its own case number and identifying the person by some name.

However, without a DCI#, DTN, or other universally accepted and understood tracking numbers, the ability for justice practitioners to understand how an individual has interacted with the justice system over time how each agency has been involved is limited. In addition, without tracking numbers tied to the information and supporting business rules, automated movement of information in the workflow will still require human intervention and in some cases actually increase the workload.

4.1.2.6.1 Creating Persistent TraCS Repository

Currently, there is no centralized place in which LEA citations or any other charging information is collected. TraCS passes citations to the ICIS and the Courts through a file server at DPS simply used as a mechanism to move the information. These electronic exchanges currently happen from the local agency's TraCS system to DPS, with the paper citation generated by TraCS moving directly to the Court. The creation of a centralized repository to receive this information would allow for a broader use of TraCS, allowing other agencies access to the information over a longer period of time. Centralizing key components of the exchange information would also increase the robustness and reliability of using TraCS for real-time exchanges, including the assignment of important tracking numbers to facilitate traceability throughout the criminal justice process.

Options

1. TraCS should develop a central repository of all charges initiated in Iowa, both those initiated in TraCS as well as those that are generated from other LEA or Sheriff RMSs.
2. Continue passing charges from local law enforcement agency to local Court.

Recommendations

TraCS should develop a central repository of all charges initiated in Iowa, both those initiated in TraCS as well as those that are generated from other LEA or Sheriff RMSs.

Benefits

This was recommended in a recent evaluation of the Electronic Citation Component conducted for the Department of Transportation by CISCO. This recommendation, with which the MAXIMUS/URL Team agrees, encourages the movement from a file-based process to a transaction-based process and will provide a more reliable ECCO data integration solution by taking advantage of the built-in features of the Oracle database. TraCS Agency Workstations and ICIS will connect to this database to send and receive ECCO information.

4.1.2.6.2 Provide DCI# Back to Sheriff/LEA as Soon as Booked on AFIS

Traceability in Iowa would be enhanced if the DCI# was also included on the charging documents.

Options

1. Create a message through the IOWA System to notify the booking agency that fingerprints have been taken and a DCI# is assigned.

Recommendations

DPS will provide the originating agency the DCI# of the individual fingerprinted as soon as a number is associated with the DTN. If this is done in a timely fashion, the LEA will put the DCI# on subsequent charging documents exchanged with the County Attorneys, the Courts, or even DPS.

Benefits

This modification will further expand traceability in Iowa and facilitate the ability to track incidents, cases, and persons through the criminal justice process.

4.1.2.6.3 Expand DTN Concept to all Charge Initiation Events

Currently, the DTN is not assigned when there is no fingerprint. This limits traceability in the current system, especially for traffic cases, where no fingerprint is collected. Neither the DTN nor the DCI# appear on the charging documents used in the course of prosecuting a case.

Options

1. Expand DTN concept to all charge initiation events, both fingerprint and non-fingerprint supported, while ensuring that the use of the DTN and DCI identifiers will in no way be compromised.
2. Continue assigning the DTN only in cases in which fingerprints are collected.

Recommendations

The Greensheet can be eliminated if an individual, when booked, is assigned a DCI# and DTN and these are incorporated into the LEA and prosecutor charging documents, such as those generated by TraCS. If the individual is not booked, a DTN would be generated (even if it was known not to be linked to a fingerprint). Non-traffic Complaints should contain similar demographics as traffic, like DL#, and other data elements usually found on a drivers license. It would be important to take measures to ensure that the DTN and DCI identifiers are not compromised.

Benefits

This will allow the Courts to issue warrants from the information passed via the charging instrument.

4.1.2.6.4 Complaint and Affidavit Standardization

Currently, there is no consistent process within the State regarding the Complaint and Affidavit forms used by law enforcement for a non-citable offense. It has been

documented in the previous studies (URL Adult Exchange Analysis) that these forms should be standardized. Currently, there is an effort in TraCS to standardize the Complaint.

In addition, a standard process could also include the consistent assignment of important identifiers (DTN) to promote traceability throughout the justice system in Iowa.

Options

1. Leverage and expand current TraCS standardization effort.
2. Include Affidavit information on the Complaint to promote e-filing

Recommendations

For indictable offenses, the Complaint form should be made available with the additional information required for the Affidavit. In most cases, there will be an arrest and booking with an indictable offense; however if no DTN is available, a similar process as described above will be necessary.

Benefits

The standardized process and inclusion of important Complaint information for the Affidavit will promote electronic filing and traceability in Iowa. It will also reduce the burden on the Courts by not requiring them to accept incomplete information or information that varies by the filing agency.

4.1.2.7 Other Exchanges

4.1.2.7.1 Implement Automated Warrants Exchange

A high priority identified in the URL Integration Adult Exchange Analysis in Iowa is the ability to exchange warrant information in an automated fashion in real-time. This was piloted with some success with the Linn County Sheriff.

In order to realize this exchange, there are several business process-related issues that will need to be addressed, such as the record quality (completeness) for warrants, the court clerk's ability to review and enhance records, and how the exchange will be supported and responsibilities shared by DPS and the Judicial Branch.

Options

1. Expand the Linn County effort to facilitate broader exchange of warrant information.
2. Conduct business process review to identify ways the current barriers to automated warrants exchange can be overcome.
3. Overcome the disparate security policies between DPS and other systems by replicating the process used to exchange protection order information.

Recommendations

The process which has proven successful with protection orders should be employed for warrants issued by the Court. The lessons learned from both the protection order process and the pilot between the Court and the Linn County Sheriff will provide the guidelines for maintaining synchronization. If the Courts are provided more complete information on the charging documents as suggested above the warrants from the Courts should meet all NCIC requirements.

Benefits
The automated exchange of warrant information has been identified as a significant business priority for justice practitioners in Iowa.

4.1.2.7.2 Court Dispositions Provided Real-Time to Exchange Partners

Many agencies would benefit from receiving the Court disposition in an automated fashion upon its rendering.

Options
1. Provide disposition information real-time through the proposed CJIS Broker.
2. Leverage the GJXDM to support this transaction.
3. Expand ability of key systems (ICIS, ICON, CCH) to accept digital signatures.

Recommendations
We recommend all of the options above. Court case dispositions should be provided electronically to CCH, DOC, and Jails. Both DOC and Jail should receive style sheet representation with electronic signatures. The orders – disposition and sentence – should have standardized data, along with the body of the order (free text). The design style sheet of an order would be flexible within reason and determined by a collaborative process.

Benefits
Information about Court dispositions would become immediately available to partner agencies.

4.1.3 Assess Risk to Implementing Business Process Change

Iowa's current justice environment has made significant strides over the past several years in developing strong working relationships between the State agencies. This has resulted in a Memorandum of Understanding between the Judicial and Executive Branches. The MOU has set up a CJIS Advisory Board made up of both local and State representatives. The Advisory Board is guiding the arduous task of integrating Iowa's varied and disparate justice information systems.

The CJIS effort in Iowa is not just beginning with this project to develop a strategic plan, but has been evolving through a series of studies and projects geared toward gaining a better understanding of the complex business practices in Iowa and, in several cases,

implementing projects to address specific business needs. For many years the Executive Branch, through the Department of Public Safety, sought to automate the matching of arrest records and Court dispositions. To date, many states still use a manual process to update criminal histories. Iowa was successful in this project and maintains one of the higher automated disposition matching rates in the country. There have been many other gains mentioned in the body of this section for which both State and local officials should take pride.

However, as a part of the goals the justice community has set for itself over the last several years, coupled with the findings from the various studies that have been undertaken, the current environment highlights how much work is yet to be accomplished. The As-Is section of the plan set out to define a baseline from which the gaps between the goals and the current environment could be understood. Several key observations were made:

- The State has a very robust Justice Data Warehouse that is limited only by the lack of integration between the feeder agencies/branches
- The State systems share information with each other, but this is primarily for the purpose of populating individual data warehouses to be used by the agency's/branch's stakeholders alone.
- There are diverse business practices in the justice community at the local level.
- Documents shared between agencies vary from jurisdiction to jurisdiction, but there is movement to standardize some of these forms.
- There are very few transaction based exchanges. Where there are such exchanges they are successful but are currently held back by the technology employed. In addition, the successes have not been used as spring boards to other similar, but perhaps more challenging, exchanges.
- The State agencies maintain unique representations of data that in some form all of the agencies do or could maintain. Examples of this would be name representation, demographics, and identifiers.
- The local agencies have disparate systems but do share common applications (TraCS) or are moving in that direction (County Attorney Case Management Systems).
- The justice leaders and practitioners, for the most part, have expressed a willingness to adjust their systems and practices to accommodate the CJIS initiative, which is seen as for the greater good.

The review of past studies, interviews with the State agency representatives, and the survey results all show the limitations of the current level of integration in Iowa. However, they do show how the strengths which are necessary to build a successful integrated justice information system and cognition of what it will take to move forward.

4.1.3.1 CJIS Implementation in Iowa

As suggested above, there are several external influences that will dictate how the CJIS Integration Plan is implemented in Iowa. These external influences include the ability to create and sustain a governance and project management structure to support the initiative, as well as the ability of that structure to seek support from outside decision makers and funders to support the effort.

The MAXIMUS/URL Team have made several recommendations about the Project Management and Governance of this initiative. We believe that there are important issues that ask how, who, and where the CJIS effort will be implemented that are critical for the Advisory Committee and Governance Board to address as part of its legislative package for CJIS implementation and in advance of any procurement to implement the Strategic Plan.

In Section 4.1.2.1 above, we discuss the importance of establishing this project management structure and giving it ample authority and resources to lead the CJIS implementation in Iowa. Examples of specific responsibilities with which it should be tasked include:

- Conducting outreach with other State and local policymakers and justice practitioners to promote the CJIS vision statewide;
- Coordinating local/other State implementations and ensuring adherence to the plan;
- Garnering funds (both federal and state) from other funding agencies to provide as much financial support for CJIS in Iowa as possible;
- Writing grant proposals and conducting other fundraising activities in support of CJIS implementation in Iowa;
- Overseeing business process-related improvements, such as forms and business process standardization;
- Overseeing technical collaboration efforts, such as XML schema development and the establishment of meta-data standards and common data value elements;
- Managing any external contractors or vendors brought in to assist with CJIS in Iowa; and
- Creating and managing project plans associated with CJIS implementation.

In addition to a proactive governance and project management structure, it is clear that the CJIS Advisory Committee and Governance Board will need to seek legislative support for the strategic plan and its implementation. As have been previously identified, there have been several policy issues around sharing of information (especially juvenile information sharing) that must be clarified by the legislature. In addition, there are implementation issues that must be addressed, as well as the nexus between CJIS implementation and other public policy priorities in Iowa. Examples of a structure for a legislative package would include:

Information Sharing Issues

- Issues regarding prosecutor charging behavior need to be addressed; Iowa Code and Court Rules to a certain degree enable this variability in behavior;
- Provide authority to pass digital representation of signature along with document to allow for e-filing and electronic orders;
- Confidentiality issues regarding the sharing of PSI information;
- Juvenile fingerprinting and the confusion in Iowa law around the issue of custody and whether it is a criterion for printing juveniles; as such, the policy should be reviewed. Improved fingerprinting of juveniles will also improve disposition reporting to the DPS; and
- Especially in the juvenile justice system, public policy issues about the treatment of juvenile information must be addressed before automation can occur.

Governance, Implementation Issues

Consistent with the MAXIMUS/URL recommendations listed above, a legislative package would need to address the following with regard to CJIS governance and implementation:

- Issues regarding legal ownership of data within the CJIS enterprise must be addressed;
- Organizational issues regarding where CJIS is maintained and how it is managed must be established before implementation can begin;
- The successful governance structure that has been established must be revisited and expanded to support CJIS implementation; and
- The legislature should also address the role of CJIS in other high-priority legislative initiatives, such as the need to study information sharing around sex offenders and the creation of the Chief Information Officers (CIO) Council.

Funding

- Requesting an annual appropriation for CJIS activity in Iowa and requesting that appropriation be administered through the CJIS office;
- Requiring that all federal and state grant funds for justice technology be spent on projects and activities consistent with and in furtherance of the CJIS strategic plan;
- Authorizing the Executive Branch to develop an interagency budget proposal to support projects related to justice information systems integration;
- Holding joint hearings of budget, finance, and relevant oversight committees on integration plans and budget proposals;
- Creating a joint House and Senate technology committee, or, alternatively, a technology committee in each chamber with jurisdiction over projects and spending proposals related to state agency information systems; and

- Establishing a "special technology account" to finance initiatives related to State agency information systems.[29]

In Section 5 of this document, the MAXIMUS/URL Team provide more recommendations and detail about these implementation efforts and the costs associated with achieving integration in Iowa, and associate them with a projected five-year timeframe.

4.2 To-Be Technical Environment

The Iowa CJIS Integration Plan RFP requires defining the appropriate technologies necessary to integrate State and local criminal justice information systems and related databases. The To-Be Technical Environment addresses the technical components that will need to be implemented in the five-year State of Iowa CJIS Integration Plan. The MAXIMUS/URL Team created a benchmark of the current state of technology regarding its adoption as well as its current capability to participate in an integrated environment. The recommendations in the following section are intended to establish an environment that facilitates the automated exchange of information based upon this benchmark.

The As-Is Technical Assessment illustrates that Iowa, as well as many other states, has a disparate level of technology and integration capability, especially at the local agency level. The use of technology ranges in the Iowa justice community from very robust applications to jurisdictions without any information technology capabilities. The To-Be technology requirements must address this gap to ensure that each can benefit in the integration effort and ensure there is synchronization between manual and automated processes over the transition to a fully automated justice process. The following principals were used to assist in making these recommendations:

- The technology must help achieve the benefits of integration expressed in section 3.2.A of the State of Iowa Criminal Justice Information System Integration Plan Request for Proposal;
- State of Iowa Technology standards should be incorporated wherever possible;
- The recommendations should have as little impact as possible upon the current business solutions being utilized by justice practitioners in Iowa;
- The recommendations should leverage existing infrastructure and capability in the current Iowa technology environment;
- Best practices from national organizations, federal agencies, other states and localities that are addressing the justice integration issue should be used where applicable; and
- Technology recommendations should achieve a business goal and not be simply for the sake of the technology.

[29] *Optimizing State Investments for Justice Information Sharing: NGA Issue Brief*, National Governors' Association, 2002, page 5.

The To-Be Environment has the following highlights as documented in the remainder of this document:

- Adoption of a service-oriented architecture, as mentioned above, as a key premise to the CJIS Solution in Iowa;
- Implementation of a centralized Iowa CJIS Broker to facilitate information sharing between information sharing partners;
- Utilization of the ICN as the Iowa CJIS Solution network backbone where allowable by state statute; and
- Adoption of GJXDM as the State's data standard for information exchange.

4.2.1 Integrated Enterprise Description

The objective of the Iowa CJIS initiative is to provide an infrastructure that allows the disparate justice application currently deployed to share critical data in an accurate, complete, and timely manner. The infrastructure must provide this functionality with as little impact as possible upon the current application solutions being utilized for support of the participating agencies business processes. Several models supporting a distributed computing environment exist that could be adopted for use in the State of Iowa CJIS Solution.

Options

1. Adopt the Common Object Request Broker Architecture (CORBA). CORBA is a language-neutral distributed infrastructure that allows programs written in C, C++, Java, and even COBOL to communicate across networks.
2. Adopt Remote Method Invocation (RMI) architecture. RMI is a Java-based technology that allows Java programs to exchange data and trigger remote method calls across Java networks.
3. Adopt Component Object Model+ (COM+) architecture. COM+ is a Microsoft-centric technology and allows Windows platforms to communicate with each other.
4. Adopt a service-oriented architecture (SOA). SOA is also a language-neutral distributed infrastructure that allows one entity (computer) to perform a defined measurement of work on behalf of another entity across a distributed computing environment regardless of the system platform.

Recommendation

The MAXIMUS/URL Team recommends the adoption of the SOA model for facilitating complete, accurate, and timely information sharing in the Iowa CJIS environment. The SOA model provides the Iowa CJIS initiative greater flexibility than any of the other options. It establishes a open architecture environment for information sharing independent of the computing platforms deployed in that environment and has widespread support in the criminal justice community. The SOA model is the

recommended approach of the Global Infrastructure/Standards Working Group[30] and was unanimously selected by Global Justice Information Sharing Initiative (Global) Advisory Committee as a framework for achieving justice integration.

Benefit
An SOA approach will provide the greatest flexibility to the Iowa CJIS initiative for sharing information. SOA provides the following benefits to achieving the Iowa CJIS initiative:

- Driven by integration of the business processes
- Open
- Reusable
- Cost effective
- Minimizes impact on partners
- Enhances the management of the growth in the number of interfaces

The SOA approach will focus on leveraging existing information exchanges currently in the state, but allow exchange partners to upgrade or modify their own systems as necessary to meet their own business goals.

Most importantly, Iowa justice practitioners will not be required to port their current solutions to a new platform, and new solutions will easily fit into the model. The architecture provides full support of Microsoft, Linux, UNIX, JAVA and Mainframe in addition to many other application platforms. Several of the other options available either require the platforms to be homogeneous, which is not a realistic and would be an extremely expensive endeavor. Additionally, the SOA approach is consistent with the other Iowa CJIS Integration Plan requirements to support web-based technologies. An SOA can easily incorporate web services SOAP, WSDL and UDDI, but is not exclusively tied to these types of solutions.

Other methods of information sharing across networks using structured data have a place in an SOA environment and can be utilized to achieve the real outcome of integration which is information sharing and not web service deployment. An SOA supports loosely coupled integration that will allow any of the participants to upgrade or implement new systems without affecting the overall functionality of the enterprise or require negotiating new data sharing agreements with information sharing partners. This can be particularly beneficial when a partner in an information exchange wants to modify their system capability, but their information sharing partners are not prepared or do not have the resources to upgrade their own capability. Additionally, the SOA can incorporate and make use of the push, pull, publish, query, subscribe, and notification functions approach to information sharing at very rudimentary levels of integration.

[30] A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA), The Global Infrastructure/Standards Working Group, September 28, 2004.

Finally, the widespread support of the SOA model will provide Iowa a national community of other CJIS implementers to share best practices and strategic approaches. The lessons learned by others traversing the justice integration path will be a source of applicable experience to be brought to bear in the Iowa implementation.

4.2.2 Centralized Broker Description

Integration in Iowa will require enforcing standards and policy for exchanging information, the creation of an environment to host notification and subscription capabilities, and the ability to leverage as much of the capabilities of the current deployment of business applications to share information.

Options

1. Implement an application to centrally locate and manage the enterprise functions not inherent in the current application solutions.
2. Implement the policy and rules across the distributed systems and allow for local management and enforcement.

Recommendation

The MAXIMUS/URL Team believes that the State of Iowa should implement a CJIS Broker to assist in facilitation of justice information exchange. The implementation of the CJIS Broker would provide a single centrally managed area for the creation and maintenance of critical enterprise functions and business process management. State and local justice participants in the Iowa CJIS initiative would be able to re-use the capability provided in the CJIS Broker and focus their available funding for information technology systems to improve their internal business processes and not on implementing additional technology and overhead.

Benefits

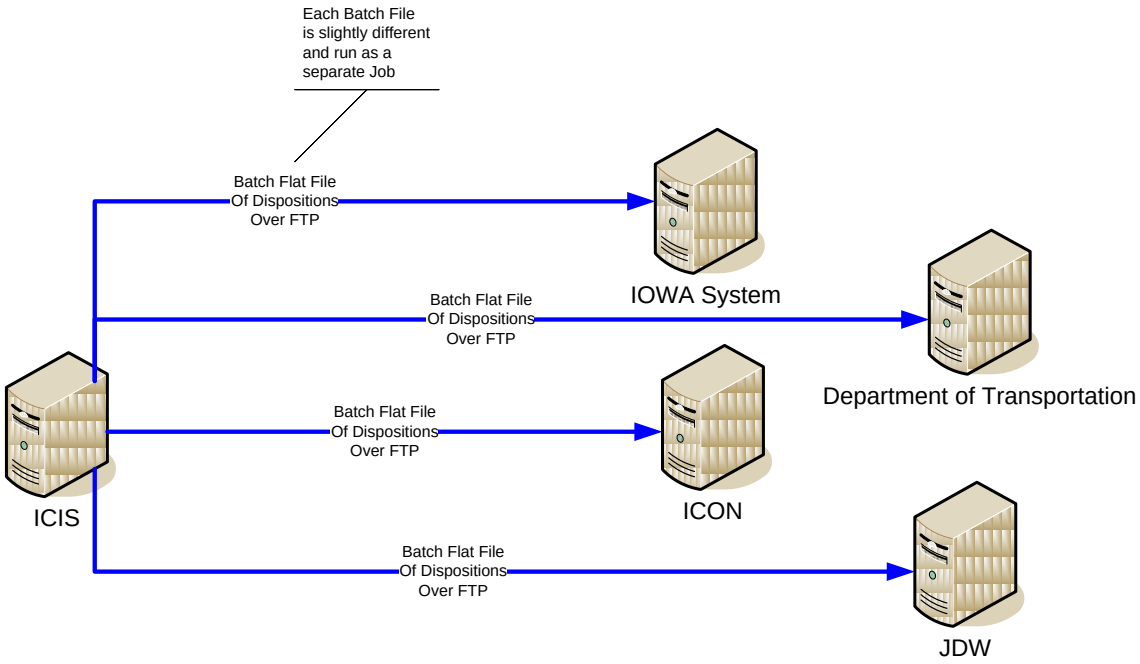
The immediate benefits of implementing the CJIS Broker to criminal justice practitioners in Iowa are that it:

- Supports independent agency development cycles
- Provides for a layer of abstraction
- Leverages state investment

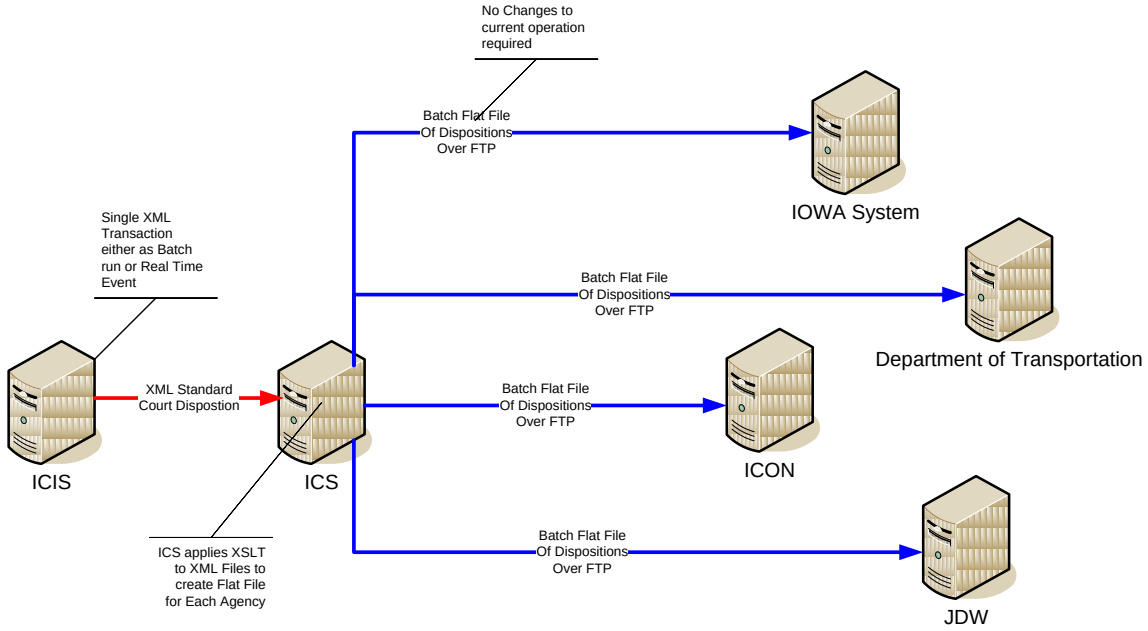
The CJIS Broker will provide each participating agency a single point to interface for exchanging information with all of their information sharing partners. This approach will relieve agencies of the burden to develop and maintain multiple interfaces which can multiply exponentially if only one additional partner is added.

Additionally, the Broker can help off-load many of the expensive processes currently being performed across the enterprise to exchange data. It has the ability to leverage a single transaction for delivery to multiple information sharing partners in multiple data formats which minimizes the processing requirements for partners. For example, the ICIS system currently shares data electronically with multiple agencies using a flat file

that is sent via FTP to each agency. Each agency's data need is slightly different and requires a separate program to extract the data from the production system. The following diagram illustrates the current paradigm.

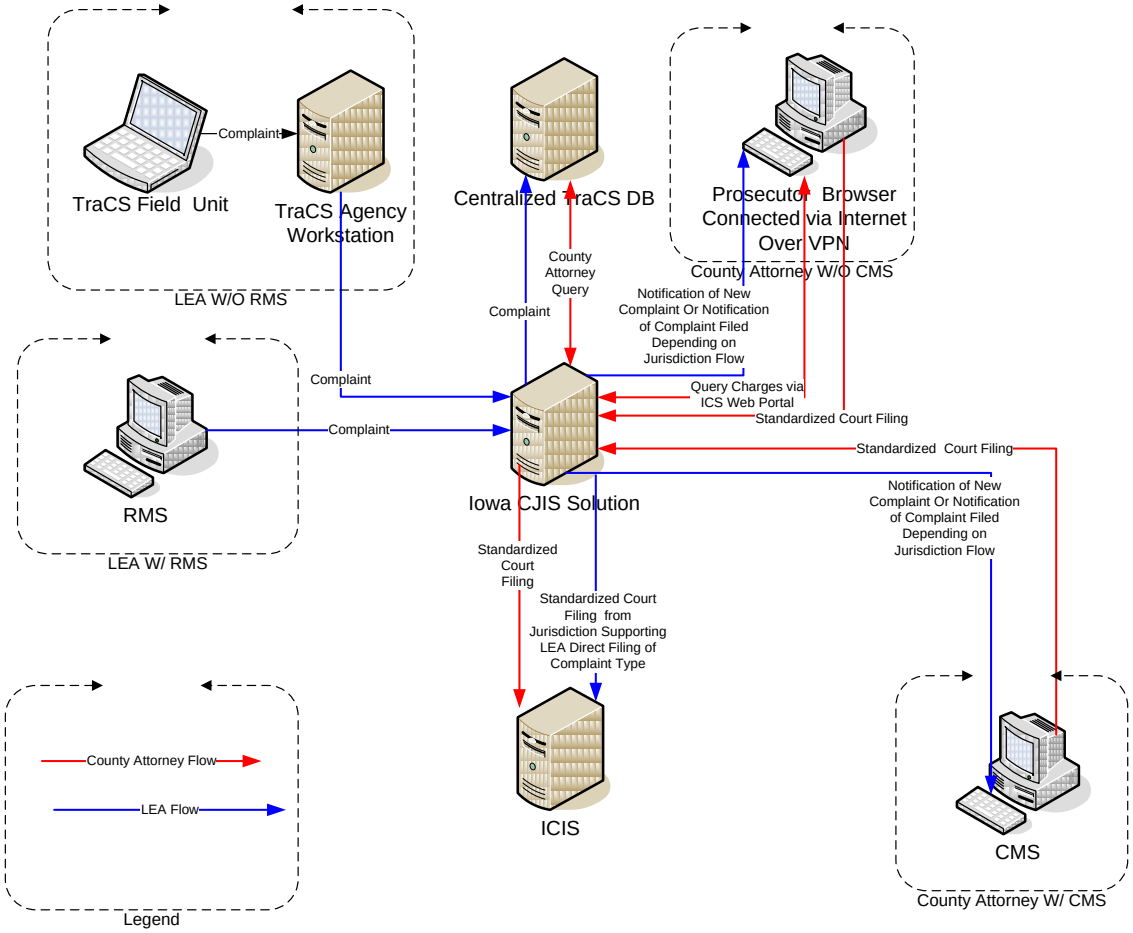


By utilizing functionality within the CJIS Broker to transform data, the ICIS system could begin sending a single file of complete information to the CJIS Broker, preferably an XML document, but not necessarily. Business rules could be applied at the CJIS Broker to transform the ICIS data into the various formats of the information sharing partners, reducing the processing requirements from four separate programs to one. If additional partners are added, the single extract program can be modified to ensure the completeness of the data and the additional work of transforming the data for the new partner added to the Broker. This approach is depicted in the following diagram.



The CJIS Broker supports a phased approach of sharing information that allows for information sharing partners to move from a batch file sharing operational process to real-time, event-driven sharing independent of one another. This concept is also illustrated in the previous diagram. By moving the exchange to the CJIS Broker, the court is able to modify its current process for creating the exchange data, but the DPS, ICON, and other sharing partners are not required to update their own programs for processing it because the CJIS Broker delivers it in the same fashion as it was previously handled by ICIS. The CJIS Broker will provide a layer of abstraction between the information sharing exchange partners, allowing for them to easily upgrade or replace their own IT systems without having the change cascade throughout the enterprise.

The CJIS Broker can also be leveraged to help fill the disparate levels of automation by providing access to the enterprise processes via user interfaces. The To-Be Business Environment seeks to leverage current data stores and application implementations to help fill this gap at the local law enforcement agency and County Attorney offices. Some of the most critical justice information exchanges within the enterprise case are those by law enforcement agencies initiating charges, and the filing decisions of those charges by County Attorneys. The CJIS Broker system could help automate these actions by leveraging the TraCS functionality recommended in the ECCO Audit performed by CISCO Inc. The following diagram illustrates how the CJIS Broker could fulfill this role:



The diagram illustrates the implementation of standard exchanges from Agencies with and without management systems with the following approach:

1. TraCS utilize the CJIS Broker to exchange "COMPLAINTS" with multiple agencies requiring the data. Single transaction could be used to populate the TraCS central repository, the County Attorney CMS, and the ICIS system when the jurisdiction allows for direct filing to courts.
2. RMS exchanging data would behave in the same manner.
3. Count Attorneys without a CMS would have the ability to query charges through the CJIS Broker, awaiting charge decisions from them on the TraCS central repository.
4. County Attorneys would use the user interface of the centralized Broker to exchange a "STANDARDIZED COURT FILING" with ICIS.
5. County Attorneys with a CMS would route "STANDARDIZED COURT FILINGS" through the centralized Broker to ICIS.

It is important to note that even if the CJIS Broker is being leveraged to fulfill automation needs in agencies where there is currently none, it is not the intention of the CJIS Broker

to replace any functionality in the current deployment of business applications. However, the CJIS Broker should help the current business solutions achieve greater business benefits than what they are currently experiencing today. For example, the role the JDW fulfills in Iowa for criminal and juvenile justice statistics is not a function that the CJIS Broker will look to replace or fulfill, but the amount of statistical information available in JDW should be significantly increased as the automated business process is utilized to also feed the data warehouse. The traceability functions of person, enterprise cycles and charges should also ensure that the data is more accurately aggregated without the use of extensive algorithms to try and make the necessary connections between information from different data sources.

All of the State level and local level applications will require some amount of modification if they are going to implement new information sharing in an SOA environment with the CJIS Broker. Few applications in the current environment are configured for real-time, event-driven transaction generation and processing. Each will need to pursue a strategy to adopt a Transaction Architecture to be incorporated into their current environment. Several options are available. At a minimum, the strategy should take the following approach:

- Easily incorporated into the current system platforms;
- Leveraging transaction processing capabilities inherent in the system;
- Eliminating redundant capabilities to be supplied by the CJIS Broker; and
- Re-using and extending strategies that are successfully sharing information in the current application environment.

4.2.2.1 High-level System Functional Requirements

The recommendation to incorporate a centralized application into the Iowa CJIS environment will allow the community of justice practitioners to address and manage enterprise business needs in one place. Previous studies and the work done in the As-Is Assessment identified several business functions that would be appropriately placed in the CJIS Broker. The existence of these enterprise business functions will greatly accelerate achieving automated information exchange in Iowa as well as assist in the synchronization of the manual and automated processes that will need to co-exist into the foreseeable future.

4.2.2.1.1 Translation of Code Values

Iowa justice practitioners, like those in many other states, have adopted information technology to help support their own business needs independent of the other IT projects going on around them. This has resulted in a variety of code values to be created to describe elements common to each system. In other words, they are using different ways to mean the same thing. For example, one agency may use the representation “BL” to indicate a person has blue eyes, while another represents the same thing as “BLU” in

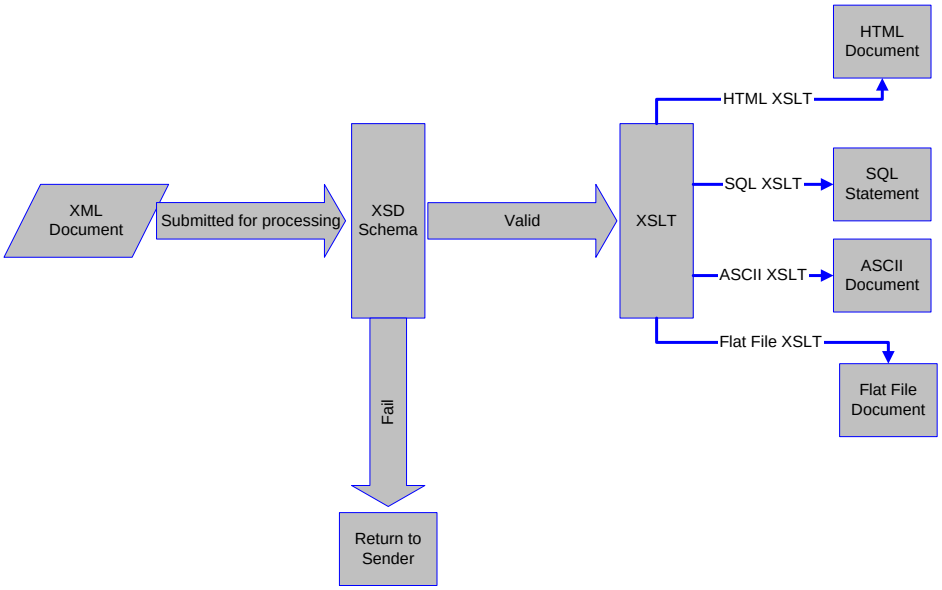
their own system. When exchanging information about a person between these two applications occurs, there must be a means to translate "BL" to "BLU" so it may be properly processed by the receiving application. To achieve this outcome, the CJIS Broker will maintain a list of enterprise values for all the common elements to be shared within the exchanges (e.g., person descriptors and vehicles). Each participant with a non-enterprise value for a particular value will "map" their value to the enterprise value. When the CJIS Broker is handling data exchanges from an agency with a translation need, it will utilize the mapping to populate the appropriate value into the message.

4.2.2.1.2 Standardized Charging Statutes

Each legislative session has potential impact upon the chargeable offenses in the State of Iowa. To ensure proper charge handling, the State of Iowa will need to develop and make available a standardized charging statutes table for implementation in each agency's management systems so unique charges can be properly identified. The County Attorney Case Management System Project has initiated this effort in their effort, and the work should be leveraged across the state. The CJIS Broker should provide a means to manage the charge statutes and distribute them to agencies needing them.

4.2.2.1.3 Transformation Services

Transformation services to facilitate communication between applications using non-standard data structures (e.g., XML to flat file) will also be needed. These services will allow for the re-use of a single transaction for multiple information sharing. A illustration of this service is depicted in the following diagram. It shows how a single XML document can be transformed using XSLT to HTML, SQL, ASCII, and flat file structures.



4.2.2.1.4 Enterprise Case and Charge Tracking Number Assignment

The need for traceability of enterprise cases and individual charges is an important business function in the integrated environment. The CJIS Broker will provide a means for requesting the assignment of these numbers at charge initiation through application and user interfaces.

4.2.2.1.5 Subscription and Notification

The CJIS Broker will provide a means for authorized users to create and maintain subscription capabilities and the resulting delivery of their corresponding notifications.

4.2.2.1.6 Logging and Auditing

The CJIS Broker will provide a means for logging and auditing of transactions it handles. Included in this capability will be transaction state maintenance for long running business processes.

4.2.2.2 High-Level System Non-functional Requirements

The CJIS Broker will consist of a variety of components including a user interface, application servers, and persistent data storage. The technology platforms to develop the CJIS Broker would be conformant with the SOA approach being recommended. Non-functional requirements at a high level are inclusive of the CJIS integration solution scalability and overall recommendations for system security. The CJIS integration solution must not only be implemented in an architecture that can scale with respect to increased transaction volume but provide for adequate load balancing and failover capabilities. Additionally, scalability must also provide for the addition of new participants in the integrated justice environment as well as minimizing the impact of growth on existing systems. System security has been addressed within the context of the network model above. However in an overall context, new procurements must also address security standards for encryption as well as the methods required by the user community to ensure the use of authentication protocols and that secured connections are established.

4.2.2.2.1 User Interface Requirements

The Iowa CJIS Solution must provide a user interface inclusive of a starting point that provides users a means to find other resources and services available. The Iowa CJIS web portal and user interface will provide a gateway where such services can be discovered by authorized users.

Options

1. Utilize an existing web portal in the state infrastructure.
2. Develop a custom solution using standard-based web technologies that meets all the needs of the Iowa justice practitioner community.
3. Purchase a COTS solution and configure it for Iowa CJIS use.

Recommendation

The MAXIMUS/URL Team recommends the Iowa CJIS solution develop a custom-built web portal and user interface specifically designed to meet the requirements of the Iowa justice practitioner community.

Benefit

A custom development of the web portal and user interface components of the CJIS Broker ensures adequate security measures and policy is applied to the web portal without creating dependencies on outside agencies or requirements for access to the gateway. Furthermore, it allows for deploying only the services necessary for the Iowa CJIS Solution without deploying superfluous and unnecessary features that are typically wrapped in a COTS approach. Finally, it provides for the web portal and user interface to be developed in the same technologies as the other components of the Iowa CJIS Solution leveraging common operating platforms and infrastructure.

4.2.2.2.2 Application Interface Requirements

The Iowa CJIS Solution must seek means to properly implement the exchange of information in an automated fashion. Multiple strategies can be employed to achieve this outcome, such as expanding strategies that are currently in use and increasing the use of web services as CJIS integration continues.

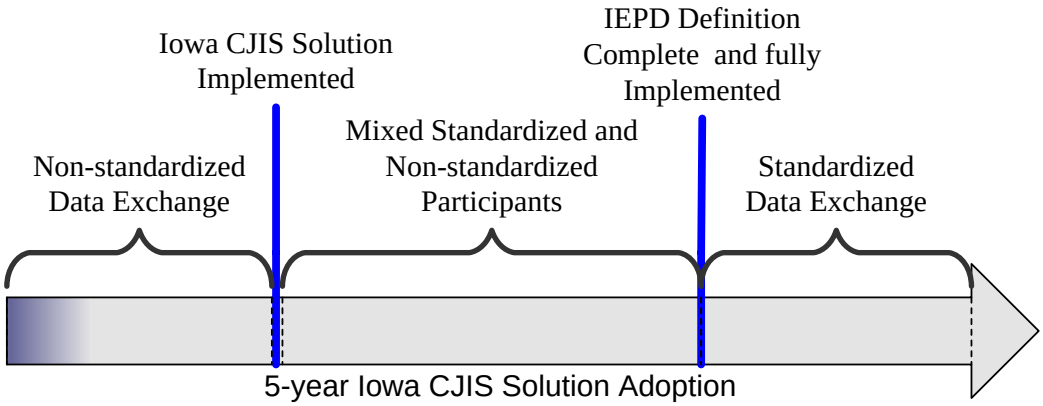
Options

1. Develop every component of the Iowa CJIS Solution as a web service with corresponding SOAP, WSDL, and UDDI components.
2. Extend the current strategies, such as FTP of batch files, to the Iowa CJIS Solution.
3. Utilize the SOA environment to leverage current application interfaces while building towards the implementation of web services supporting standardized information exchange.

Recommendation

Deploying distributed computing technologies such as web services can provide a great benefit to achieving the integrated environment sought, but these technologies must not be adopted for the sake of technology alone. In reality, the move to a 100% web services exchange environment is not a near-term achievable goal, and enforcing the approach may cause current successes to be lost. Also, over-utilization of these technologies can also provide for a management quagmire when trying to coordinate them in an end-to-end process or creating a web service that cannot be leveraged in multiple exchanges. The MAXIMUS/URL Team recommends the CJIS Broker utilize the SOA environment

to leverage current application interfaces while building towards the implementation of web services supporting standardized information exchange. The following diagram illustrates the phased approach of application interfaces to support information exchange as part of the Iowa CJIS Initiative.



Currently, information exchange is taking place in Iowa between justice practitioners' applications. These exchanges are typically non-standardized data exchanges. With the implementation of the CJIS Broker and the development of standardized exchanges through an IEPD approach using SOAP, UDDI, and WSDL components, the CJIS Broker environment will support both standardized and non-standardized exchanges. Finally, when all current exchanges have been forced because of business reasons to move towards standardization, all information exchange among Iowa justice practitioners will be in standardized Information Exchange Packets (IEP).

There may always exist components of the CJIS Broker system that are not web service enabled. Developing every component of the CJIS Broker Solution as a web service would add an unnecessary level of complexity and cost to the development and operational support of the application. Additionally, the functions of support selected for web services should be built at a level of granularity to provide the greatest benefit and easiest maintenance that can be achieved. Defining the appropriate level of granularity for creating services will be an important task in the project. The Iowa justice community implementing integrated solutions will benefit much more from a "GET ENTERPRISE VALUE" service than they will the more granular "GET ENTERPRISE EYE COLOR VALUE" service. Solution processes of value only to the Iowa CJIS Solution will be cheaper and easier to maintain if done so in the selected procedural language of the solution platform.

Benefit

The benefits of adopting the phased approach supported by application interfaces in an SOA environment include a better return on investment for both the development and long-term operational support of the system. Needlessly moving working application

interfaces to web services will not accelerate the overall integration effort. Also, taking advantage of multiple application interface approaches will ensure that applications developed in varying levels of technology are capable of participating as is best suited to their platforms.

4.2.2.2.3 Expected Usage and Scalability Requirements

A successful CJIS integration solution must have the capacity to scale as demand for its use grows. This is most obviously addressed by the architectural design of the solution, specifically its device level implementation with respect to load balancing, failover, and clustering. However, scalability as it pertains to the addition new participants and the impact to existing systems is an equally important consideration.

To put forward a CJIS integration solution that can remain viable beyond the short term, it is necessary that the solution provide for a scalable architecture capable of load balancing, failover, and clustered solutions.

Options

1. Recommend a solution that provides for immediate processing capacity and then revisit the design at a future date to determine updated capacity needs.
2. Recommend a solution that provides for over maximum expected capacity at five years and can grow without reworking the existing configuration.

Recommendation

Option #1, while meeting short-term capacity requirements, does not scale effectively in a cost efficient manner. Therefore, Option #2 is recommended. Infrastructure necessary to implement the centralized Broker solution will require an architecture that can not only meet anticipated processing requirements over the next five years, but can offer stability in balancing high volume transaction loads, provide redundancy with failover protection at a server and network device level, and optimize utilization of acquired resources by implementing a clustered solution. Scalability is achieved primarily through the clustering of database and application servers such that additional nodes can be added to provide for greater processing capability and the handling of increased transaction loads. It is recommended that an external storage area network (SAN) be used to provide for adequate data storage capacity while offering its additional capacities for failover, growth, and performance.

It is envisioned that the ICN currently has sufficient capacity to meet CJIS integration needs over the next five years and will continue to evolve to meet future growth requirements. Existing participant systems are already poised to scale with efforts such as ICIS II, the upgrade of the Driver's License in March 2006, and the upgrade of the DPS message switch in September 2005.

The centralized broker adds an additional scalability aspect by its design: the ability to accommodate new participants at a future date. As a central repository for data exchange logic and its networked infrastructure as a data exchange communications hub, new

participants to the CJIS integration effort can make use of this architecture without undue impact on the existing user base. Additionally, as a service-oriented implementation, data exchange functionality is provided between participants through the centralized Broker acting as a layer of abstraction for such exchanges. This minimizes the impact on existing systems such that additional business logic necessary to manage data exchanges with participants is a feature of the Broker system rather than a potential enhancement burden on the existing systems. The As-Is Assessment established that all major Iowa CJIS systems already have the capacity to participate in a service-oriented architecture to some degree. It is envisioned that the effort required to fully realize those capabilities does not need to be unnecessarily augmented by the addition of managing the exchange logic for each combination of pertinent data exchanges.

Benefit
A significant requirement for implementing an effective and persistent solution is to provide for scalability as well as the capacity to handle system and network failures. Iowa gains much from such an implementation as growth requiring greater processing capacity, data storage, and network utilization is inevitable. Such architecture is more maintainable and more reliable, and future growth can be planned accordingly without the need to reinvent the existing integration architecture.

4.2.2.2.4 System Business Processing Environment Recommendations

The CJIS Broker business processing application environment will need to have the capability to support the functional requirements previously identified. The environment must support SOA methods for integrating systems and have an open architecture.

Options
1. Implement the CJIS Broker on a J2EE platform.
2. Implement the CJIS Broker on a .NET platform.

Recommendation
Both .NET and J2EE provide an environment that could support the functional and non-functional requirements of the CJIS Broker. They provide similar capabilities that can be utilized to achieve the Iowa CJIS initiative; however, the State of Iowa Information Technology Enterprise(ITE) recommends the use of their WebSphere platform, which is J2EE compliant, for the hosting mid to large size applications of a complex nature. Based upon this recommendation, and the flexibility of deploying a J2EE solution to multiple hardware platforms and any operating systems with a Java Virtual Machine (JVM), the MAXIMUS/URL Team recommends the CJIS Broker business processing environment be a J2EE platform.

Benefits
Developing the CJIS Broker in a J2EE environment will provide for several options for hosting the solution, as a J2EE solution runs on the JVM which can be deployed to an array of hardware and operating system configurations. The .NET platform does offer many of the same development features that are inherent in the J2EE platform, but only

runs in a Microsoft Windows operating system, which may not meet the availability requirements of a mission critical system like the CJIS Broker.

4.2.2.2.5 System Security Model

Security in the context of network connectivity was addressed above. Overall security in terms of non-functional requirements is also addressed. Standards related to encryption levels of existing and To-Be procured devices are important so as to remain current and not immediately out-of-compliance with both State guidelines as well as any participant-specific obligations. Additionally, connectivity by users via the Internet requires recommendations for strong authentication before initiating a secured VPN connection.

4.2.2.2.5.1 Post-September 30, 2005 Procurement Requirements

Any procurement after September 30, 2005 shall require a minimum of 128-bit encryption with NIST, CSL certification of the cryptographic module to ensure it meets FIPS Publication 140-2 for "Security Requirements for Cryptographic Modules." Any minimum of 128-bit encryption procured before September 30, 2005 does not require NIST, CSL certification until September 30, 2010.

Options

1. Recommend that all procurements be made prior to September 30, 2005 so as to delay NIST, CSL certification until September 30, 2010.
2. Recommend that all procurements meet 128-bit encryption and NIST, CSL certification of its cryptographic processing.

Recommendation

Option #1 is not viable as it is unrealistic that all necessary integration related procurements would be made before September 30, 2005. Therefore, Option #2 is recommended, whereby all such procurements will need to be NIST, CSL compliant for at least 128-bit level encryption, regardless of when purchased. Additionally, any procurements for the CJIS integrated solution will necessarily meet the State of Iowa Enterprise Security Policy Guidelines.

Benefit

Rushing to procure ahead of September 30, 2005 carries a strong risk that decisions would be made hastily and without the full vetting required to ensure that all long-term implications have been addressed. This is especially germane to server and network device acquisitions when considering adequately capacity for processing and future scalability (Section *Expected Usage and Scalability Requirements*). Additionally, such premature action would incur the additional effort of bringing such procurements up to conformance with the requirement before September 30, 2010. These issues are avoided by having procurements, regardless of date of purchase, be NIST, CSL compliant with their encryption components.

4.2.2.2.5.2 VPN Technologies

VPN mechanisms and technologies such as cryptography, key management, access control, and authentication must be incorporated. User identification and authentication can take place at the network, device, and/or application level. At a minimum, a user shall be restricted from establishing a VPN session without first being identified/authenticated by no less than a user ID and password.

Options

1. All communications shall require use of VPN mechanisms with user authentication regardless of source.
2. Remote authentication of users accessing externally to the State will require at least username/password authentication before establishing a VPN connection. All other connections will be VPN secured by firewall point-to-point configurations.

Recommendation

While both options require the use of secured VPN connections for data exchanges, all automated, transaction-driven data exchanges between systems are not driven by user interface events, and consequently, not all are suited for user supplied credentials on each transaction. Option #2 is recommended, as remote users outside of the State network infrastructure will necessarily need to connect to the centralized Broker system via the Internet. Such access would require dual-mode authentication (challenge/response) via token card to establish their secured VPN connections. Such authentication is in addition to username/password authentication. This level of authentication and encryption, namely requiring remote users to establish secured and encrypted connections to the CJIS integration solution, is put forward to protect primarily remote users connecting via the Internet (e.g., County Attorney offices) from not just transmitting data "clear text" but not unduly exposing their connections.

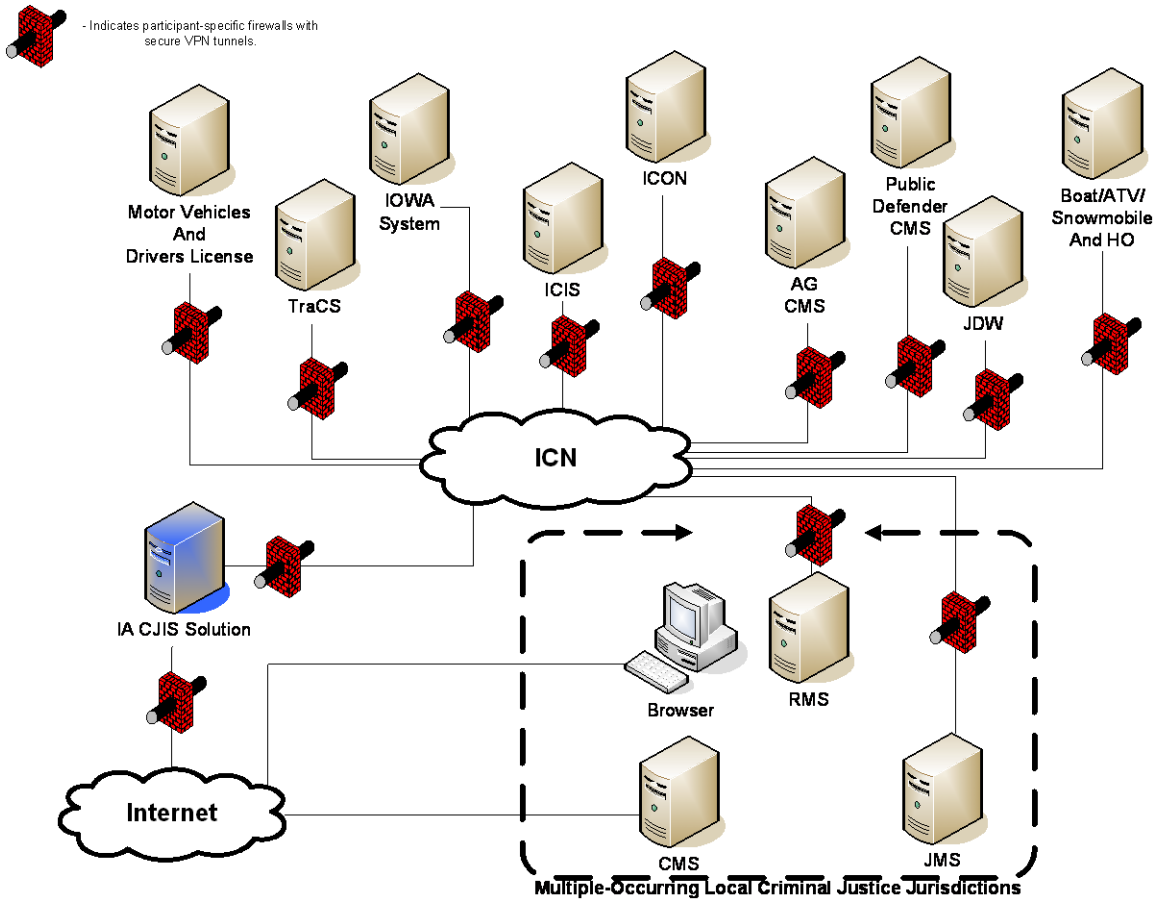
Benefit

As automated data exchanges do not necessarily require a user interface event to trigger, the recommendation alleviates individual user authentication (where unnecessary) to promote efficient exchanges. However, VPN connections that are the result of transactions initiated via the Internet would necessitate individual authentication. Here, the use of secondary dual-mode authentication would further secure the access beyond username/password authentication and consequently provide better control over the initiation of a secured connection.

4.2.3 To-Be Network Model

The To-Be network model puts forth the design of the CJIS integration solution in the context of statewide connectivity between all participants. Key to this structure is the centralized Broker that is responsible for routing data exchanges, accurately applying specific business logic to the exchanges, and offering an important layer of abstraction to

the integration solution, whereby existing systems do not need to individual manage their specific exchanges with other participants. Other key issues in the network model are the utilization of the existing ICN wide area network (WAN); secured connections via data encryption, VPN tunneling, and implementation of participant-specific firewalls; and protocol recommendations. The following diagram provides a graphical representation of those key features:



4.2.3.1 To-Be Network Communication/Connectivity Requirements

Network communication and connectivity issues are important when addressing an integrated environment that by design interconnects multiple participants in different combinations of data exchanges. Recommendations are made to high-level issues regarding communication protocols, secured transmissions, and tools requirements for participants.

4.2.3.1.1 Transfer Protocols

It will be necessary for the network facilities to support a variety of protocols, including FTP, SMTP, HTTP as examples.

Options

1. All available transfer protocols will be presented as viable.
2. Only certain transfer protocols will be recommended as viable.

Recommendation

Option #1, while very flexible and the least restrictive, is too broad of an approach to take, especially when considering the effort to manage the multiple network connections necessary in the Iowa integrated justice environment. Only data transfer mechanisms that make sense in meeting the other non-functional requirements are recommended. For the service-oriented architecture proposed for the centralized Broker solution, this will primarily mean TCP at the network level and HTTPS for the application processing, as each data transfer protocol will need to be secured. Existing data exchanges done by file transfer that would potentially still exist initially but be dropped in subsequent phases would be done with SFTP instead of FTP, while web-enabled portions of the application (i.e., data exchanges based upon user interaction via the portal functionality of the centralized Broker) would use HTTPS instead of HTTP. SMTP (e-mail) is not recommended for defined data exchanges even though it can be secured in its transmission; the nature of its design to carry free-form, unstructured message text is less formal and allows for potential ambiguity in the structure and content of the exchange.

It is understood that specific network protocols other than TCP could be necessary, especially considering direct data exchanges with existing mainframe systems. However, the overarching principle is that such exchanges are considered secured and the network connectivity manageable. The use of proprietary data transfer protocols that would not necessarily be widely available to the CJIS community is not recommended.

Benefit

By having a defined and minimal set of secured transfer protocols in use, the overall manageability of the data exchange mechanisms becomes easier and more straightforward. Additionally, with the use of commonly available protocols, CJIS community members are not necessarily restricted or "locked" into a specific vendor solution simply by the recommendations of this plan.

4.2.3.1.2 Network and Security Tools

Appropriate communications, connectivity, and security tools, (e.g., intrusion detection and token authentication) must be used to enable communications, connectivity, and security between systems and interfaces.

Options

1. The plan would recommend that all entities participating in the CJIS integration effort use whatever network and security tools that they feel are appropriate or have readily at hand.
2. The plan would recommend that a rigid set of network and security tools be used.

3. The plan would recommend functional categories of network and security specifications. Participants would need to show that the tools and infrastructure utilized are meeting minimum criteria for secured access, efficient network functionality, etc.

Recommendation
Option #1 is irresponsible and does not ensure that a consistent set of connection and security criteria will be applied across the board. Option #2 does just that but remains very inflexible and could easily hamstring a participant with impossible requirements or impose requirements that conflict with other equally valid obligations. Option #3 above is the most viable recommendation, as the larger participants already have network and security solutions in place that effectively meet existing (and future) connectivity and security requirements. Additionally, smaller participants or those fairly new to automated justice data exchanges might be unable to meet a rigid set of tool specifications without becoming disenfranchised.

Benefit
Any tool recommendations cannot invalidate the established practices of participants that are accountable to security and network requirements outside of this plan. The DPS is a prime example of this with their need to conform to NCIC requirements and IOWA System Rules and Regulations. Additionally, participants such as county and private attorneys must have some flexibility in their ability to procure and maintain communications and security tool sets.

However, a recommended set of connectivity and security tools must meet the overarching guidelines established for justice data exchanges within the State of Iowa. This approach allows for a balance to be struck between the abilities of the participants and the very real needs of the State to ensure that the integration infrastructure is not a haphazard collection of network and access devices. Such needs might necessarily dictate a single type of remote access authentication (e.g., token card) while also allowing for different firewall types for participants.

4.2.3.1.3 To-Be Security Requirements

Secured transmission of data exchanges is a fundamental requirement for CJIS integration functionality. With respect to the security of transmissions in the context of network connectivity, encryption and authentication of participants are key. These recommendations address encryption requirements and secured connectivity through VPN tunneling within the context of network communications.

4.2.3.1.3.1 Encryption Requirements, Compliance with FIPS 140-2 Specifications

All communications between participants in the integrated justice environment need to be made securely. A minimum of 128-bit encryption is considered standard as well as compliant with FIPS 140-2 specifications. This level of encryption is to be considered minimum as future requirements beyond 128-bit are a reality in the short term.

Options

1. The plan will not address this specifically, as most of the communications from the larger participants already use 128-bit encryption.
2. A minimum encryption level of 128-bit is necessary for all exchanges not originating within the State communications backbone (i.e., County Attorney offices). However, those originating in-state can accept the ICN communications as already protected.
3. The plan recommends specifically that all communications in the integrated justice environment utilize a minimum 128-bit encryption regardless of origin.

Recommendation

It is fundamentally important that all data exchanges are transmitted in a secured environment. Therefore, the only feasible option above is Option #3. Currently, not all data exchanges are encrypted and do not treat the use of the ICN as trusted. It is important that in moving forward with CJIS integration that all data exchanges meet a minimum 128-bit level of encryption.

All connectivity that originates outside of the State network like County Attorney offices utilizing the Internet to access the centralized Broker system, must do so using secured and encrypted VPN connections validated by dual-mode, token authentication and username/password .

Benefit

The benefits to not transmitting justice-related data as "clear text" are fundamental. This information, especially with respect to juvenile data is necessarily considered as well as required to be protected and to be used only within the context of sanctioned criminal justice business processes. By recommending the use of at least 128-bit encryption, a sufficient level of data protection is put forth as a baseline without unnecessarily restricting users that are required to use higher levels of encryption.

4.2.3.1.3.2 Firewalls

Firewall implementation must be in place to ensure a clear segregation of justice related data exchanges with other traffic over the ICN.

Options

1. Rely solely on the existing ICN firewalls that segregate ICN traffic from the raw Internet traffic. This implies that data transmissions over the ICN can be considered trusted.
2. Implement firewalls specific to each participant or groups of participants as well as for the centralized Broker system to ensure that point-to-point, secured tunnels are established for data transmission over the ICN.

Recommendation

Option #1 is not feasible as the ICN is not solely dedicated for use by the Iowa CJIS community. It will be important to ensure that all automated, transaction-driven data exchanges between systems utilize a secured VPN tunnel between the participants and the centralized Broker system. These secured connections need to be implemented by an automated, negotiated exchange between the participating firewalls that follow configurations established upfront. Therefore, Option #2 is recommended.

Benefit

The main benefit is that in order to implement data exchanges that originate from event-driven transactions as part of the business processes of the given systems, secured VPN tunnels within the ICN need be automatically negotiated. Having participant-specific firewalls with corresponding configurations to the centralized Broker firewall will allow for such secured connections to be negotiated automatically. Additionally, such connections will allow for isolation of individual IP addresses and any specific rules governing the access and connectivity of that device.

4.2.3.1.4 Identify Existing Network Infrastructure to Provide CJIS Backbone

A comprehensive network infrastructure must be in place to facilitate CJIS integration communications. Such a backbone must ideally be available to all participants and that all users have not only adequate access but also resources provided to them. Fortunately, such a statewide backbone exists in the ICN WAN. The follow recommendations address the use of the ICN both in the short and long term.

The CJIS integration solution must utilize a statewide communications backbone to provide sufficient access to all participants. Furthermore, capabilities that maximizes the reuse of existing infrastructure investments needs to be incorporated.

Options

1. Develop and implement an entirely new, dedicated CJIS wide-area network, solely for the use of supporting justice data exchanges within the State of Iowa.
2. Mandate the use of the existing ICN wide area network (WAN) to support justice data exchanges within the State of Iowa.
3. Utilize the existing ICN WAN with its current limitations placed upon extensions to local and county entities.

Recommendation

Option #1 is not recommended as the existing ICN is a current and robust fiber WAN with sufficient capability and an existing presence in each Iowa county. Creating a new statewide WAN will in support of CJIS integration efforts will only duplicate existing capabilities and infrastructure.

Option #3 is the best recommendation in the short term and presents the State with the greatest overall advantage moving forward. The State agencies participating in the CJIS integration effort as well as the Judicial Branch already utilize the ICN. Additionally, local and county law enforcement agencies have “last-mile” connections provided by

private telecommunications providers to connect them to the ICN in each county. Their use of the ICN falls under the existing relationship with the Department of Public Safety whereby DPS is the ICN customer. In recommending Option #3, County Attorney offices are not immediately enfranchised in the use of a statewide WAN for network connectivity in the CJIS integration solution (i.e., centralized Broker solution). The short- term solution is to have the centralized message Broker provide functionality via the Internet so that, for example, e-filing activities, hearing notifications, and sentence and disposition exchanges are exposed as services available to the County Attorneys with existing case-management systems. The centralized Broker would provide a web browser-based application to County Attorney offices lacking case management systems or lacking systems capable of using web services.

In the short term, Option #2 is technically possible as the ICN already has a point-of-presence in each county. However, it is not immediately feasible as the ICN is prevented by law from providing services directly to local and county customers. However, in the long term, should the ICN services be extended to local and county entities, the ability to utilize the functionalities of the centralized Broker system via the ICN should then be leveraged.

Benefit
Using the existing ICN WAN is a "known quantity" for the major State agencies and the Judicial Branch already. With a point-of-presence in each Iowa county and established customer agreements with the Executive and Judicial Branches for use by the CJIS community, significant use of existing technologies is achieved. Local users in each county already have ICN connectivity by virtue of their "last-mile" connections to the ICN point-of-presence. To realize the full benefit of the ICN however, it will be important to help bring its capabilities to the local and county level in the long term.

4.2.4 To-Be Data Standards

A flexible yet comprehensive set of data standards drives the specifications of the data exchanges. It will be important not to specialize this effort with a custom and proprietary data standard that, while ultimately workable within the State infrastructure, effectively limits the State's ability to efficiently share information with other out-of-state participants. Using a global standard such as GJXDM as the baseline for developing an open and workable data standard is key. Such an effort must be put forward across the board with the To-Be data standard being used exclusively for all data exchanges.

A uniform and enterprise-wide data standard in the implementation should be addressed in the Iowa CJIS Plan.

Options
1. Implement an Iowa-specific data standard using a custom format for structuring all data exchanges.

2. Implement a collection of Iowa-specific Information Exchange Package Definitions (IEPD) that are GJXDM-conformant as the structure for all data exchange formats.

Recommendation
Option #1 is not viable as the development of an effectively proprietary data standard is not tenable in the long term and serves to potentially isolate the State with respect to other state and federal data exchanges. Option #2 is recommended as it uses a global standard, GJXDM, as a comprehensive baseline upon which Iowa can further extend to develop a data standard matched to its data exchange needs. This is more aptly put forward by the development of IEPD conformant with the GJXDM that is then utilized in the development of specific documents for each data exchange. This ultimately provides Iowa with the means to develop specifications for each exchange that provide further details on message handling and structure.

Iowa will necessarily need to define the subsets of and any extensions to the full GJXDM schema for their own business needs that may not be included in the GJXDM. For example, consider the effort to develop a unified case-filing data structure for the County Attorney offices. The use of Legal XML in this effort (specifically, the Iowa County Attorney-specific IEP definition) would necessarily need to fit into the larger Iowa State-specific XML namespace as well as meet conformance with GJXDM elements. The elements defined in the Iowa namespace should be available for re-use in the development of other IEPDs to ensure consistent descriptions of the same data and acceleration of the IEPD creation.

Benefit
Utilizing GJXDM as the baseline data standard gives Iowa a long-term advantage by utilizing a comprehensive and existing data structure accommodating the incident, individual, and case-based nature of an event's full life cycle. By proceeding under the GJXDM umbrella exclusively, data exchanges (inclusive of e-filings) can be developed into specific exchange documents and ultimately specifications that map upwards to the Iowa State-specific data standards model with defined subsets of and extensions to the GJXDM schema. All Iowa criminal justice data exchanges are then soundly based on a global model for data standards that positions Iowa for far more efficient communications with other federal and state entities rather than impose a more proprietary standard for other entities outside of Iowa to follow.

5 Strategic Integration Plan

The Strategic Integration Plan section will provide detail to the approach, rationale, and funding sources in the five-year plan for achieving the CJIS initiative in Iowa.

5.1.1 Approach and Rationale

This section will identify a standard CJIS approach customized to meet the Iowa specific CJIS implementation. Industry best practices, as well as endorsed methodologies already in use in Iowa, will be assessed and their ability to meet the objectives of the CJIS initiative identified. A recommendation for best approach will be provided.

The approach that the MAXIMUS/URL Team has taken in formulating the strategic implementation plan focuses on leveraging existing systems and incremental implementation, using proof of concepts and pilots to demonstrate results quickly and create infrastructure for future development.

The following are specific assumptions about our approach to the implementation strategy and this document:

- The strategic plan is based on current systems: the CJIS plan is intended to facilitate the exchange of information between existing systems and in no way replace their functionality;
- The order of activities in Years One through Five are important and based upon our best analyses of the necessary infrastructure that must be created early on, and as such, there are dependencies between and among tasks. In other words, tasks cannot be pulled out randomly or disregarded without there being a possible ripple effect upon the expected outcomes of the plan as it is written;
- In the cost section of the document, we have defined a low-end and high-end estimate. The labels of "low" and "high" are not intended to denote a superior solution; rather they are referring to the cost of the category. Typically additional cost adds additional performance for the category denoted, but the requirement for that performance in the Iowa CJIS solution should be driven by the detailed requirements;
- Budget estimates include operational and labor costs, in addition to hardware, software, and maintenance costs;
- While the MAXMIUS/URL Team has compiled a great deal of information about grants and funding to support CJIS efforts, it is essential for an implementation of this scale to be supported at the State and local levels. We strongly encourage the CJIS Board and Advisory Committee to work with the Iowa Legislature in preparing a budget request for general fund support to support ongoing CJIS implementation.

5.1.2 Prospective Funding Sources

An important role for the CJIS Program Office will be to advocate for grants and other funding to sustain its role of supporting local justice information sharing efforts. A consistent funding stream is critical to support the implementation of the CJIS strategic plan, assist local information sharing initiatives in complying with CJIS architecture and security standards, and ensure consistency in the areas of training and outreach to encourage support for the CJIS effort.

To date, significant grant funds have been leveraged to support the CJIS effort in Iowa. According to information provided by the Office Criminal and Juvenile Justice Planning, a total of $2,123,969 has been spent since 1999 on CJIS-related studies and pilot initiatives, including the current development of the CJIS strategic plan.[31] While receiving this funding would be a great achievement for CJIS, available grant funds are diminishing and subject to shifting policy priorities. As such, it is important for the CJIS Program Office to explore and leverage all possible funding opportunities and other program support. We strongly encourage the CJIS Program Office to work closely with the Iowa Legislature in requesting a general fund appropriation to support CJIS implementation.

5.1.2.1 Federal Funding

The U.S. Department of Justice, Office of Justice Programs (OJP) distributes millions of dollars each year to state and local agencies to support a broad array of crime control and prevention initiatives. That said, federal funding to support criminal justice efforts have declined in the past years; the Administration's Fiscal Year (FY) 2006 budget request slashes the traditional OJP funds in support of local criminal justice efforts. A presentation provided by the National Criminal Justice Association reports that the President's FY 2006 budget would propose to reduce justice assistance funding by approximately $1.3 billion from FY 2005.[32]

While OJP funding has declined significantly over the past several years, funding administered to State and local governments through the U.S. Department of Homeland Security (DHS) has increased since the DHS creation in 2002. Many of the programs funded through DHS can be used to support justice information sharing systems – some of which could provide support to the CJIS Program Office, while others could go to directly support local-level integration efforts.

[31] *CJIS Funding for the State of Iowa* (spreadsheet provided by CJJP) (hereinafter *CJIS Funding*).
[32] *A Collaborative Effort: What it Takes to Make a DEC Program a Success*, Lori Moriarty, North Metro Task Force and Cabell Cropper, National Criminal Justice Association, at www.ncja.org (hereinafter *NCJA Presentation*).

5.1.2.2 Current Justice Block Grant Programs

To date, there have been several programs that have assisted state and local agencies with the administration of justice, including technology-related programs. The Edward Byrne Memorial State and Local Law Enforcement Assistance Act Formula Grant Program (Byrne) was the largest multi-purpose grant for criminal justice administration that is passed from the federal government to state criminal justice planning agencies, and was administered by the U.S. Department of Justice, Bureau of Justice Assistance (BJA). The grant provided state agencies with funding based on a formula that can be used for general crime control and prevention activities, including justice technology and information sharing initiatives. The formula is based on factors such as crime rate and population, among others. In FY 2004, the Byrne formula grant program was funded at $500 million.

To access these funds, state agencies must submit a multi-year plan for how the funds will improve the administration of justice in the state. In the State of Iowa, Byrne funds are administered by the Governor's Office of Drug Control Policy (ODCP), which received $5,307,090 in Byrne funds in FY 2004.[33] The CJIS Program Office should seek to continue its partnership with ODCP to determine if and how information technology is a component of the overall statewide criminal justice plan in Iowa.

At the local level, the Local Law Enforcement Block Grant (LLEBG) provides direct assistance to local law enforcement agencies for equipment, technology, and other materials directly related to basic law enforcement. Funds are provided directly to local jurisdictions, but in FY 2004 the State ODCP received a small state grant in support of local law enforcement efforts in the amount of $163,125.[34]

On December 8, 2004, Congress passed an Omnibus Appropriations Bill (H.R. 4818) to provide funding for the U.S. government for FY 2005. There were significant changes in the structure of assistance to state and local justice agencies. The funding bill included language that will replace the Byrne Formula and LLEBG grants with the Justice Assistance Grant (JAG) program, which will include a broader base of purpose areas for state and local agencies to use grant funds. According to BJA, the benefits of the JAG program include:

- Awards are distributed up front instead of on a reimbursement basis, giving recipients immediate control over their funds.
- Direct recipients can earn interest on their awards, generating additional funding for future justice projects.
- Projects can be funded beyond a 4-year period, allowing successful initiatives to receive funding to continue and expand their efforts.

[33] IOWA FY 2004 OJP, OVW and COPS Grants Listed Alphabetically by City, at www.it.ojp.gov (hereinafter *FY 2004 Allocations*).
[34] *FY 2004 Allocations.*

- Fewer fiscal and programmatic reports are required, saving state administering agencies and local programs valuable staff time and resources.
- Mandatory set-asides are eliminated, encouraging states and communities to spend justice funds where they are needed most.[35]

JAG will replace the Byrne Formula and LLEBG programs with a single funding mechanism that will simplify the administration process for grantees. According to BJA, the procedure for allocating JAG funds employs a formula based on population and crime statistics in combination with a minimum allocation to ensure that each state and territory receives an appropriate share. Not all local government entities are eligible for direct JAG awards. JAG was funded at $536.5 million in FY 2005, but is eliminated in the President's budget request for FY 2006.[36] With the 2005 allocation, the State of Iowa received a $3,121,286 allocation, while 18 other local jurisdictions in Iowa received direct grants of $1,475,271 for a total allocation of $4,596,557.[37]

5.1.2.3 Other Federal Grants

Other federal funding opportunities to support CJIS Program Office Goals are under the Crime Identification Technology Act (CITA) and the National Criminal History Improvement Program (NCHIP), which offer assistance to state agencies in improving and implementing effective state and local justice information systems. The President's proposed FY 2006 budget would increase funding in this area, proposing $58.2 million for these programs, up from the $24.7 million appropriated in FY 2005. In Iowa, the DPS administers the NCHIP funds, which were allocated at $377,093 in FY 2004.

As mentioned above, there has been a significant shift in funding away from OJP to DHS. Specifically, there are three programs that may be leveraged for technology-related purposes:

- State Homeland Security Grant Program, which was funded at $1.5 billion in FY 2005
- Urban Area Security Initiative, which was funded at $885 million in FY 2005
- Law Enforcement Terrorism Prevention, which was funded at $400 million in FY 2005[38]

According to the NCJA, the President's FY 2006 budget request "proposes to restructure $2.6 billion in grants for States, urban areas, and infrastructure protection, so that DHS

[35] U.S. Department of Justice, Bureau of Justice Assistance (BJA) website, www.ojp.usdoj.gov/bja (hereinafter *BJA site*).
[36] *NCJA InfoLetter*, National Criminal Justice Association, February 7, 2005 (hereinafter *InfoLetter*).
[37] *BJA site*, State of Iowa allocation.
[38] U.S. Department of Homeland Security (DHS) Fact Sheet: Department of Homeland Security FY 2005 Appropriations Act, at http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0541.xml.

will target grants to fill critical gaps in State and local terrorism prevention and preparedness capabilities, taking into consideration their threats and vulnerabilities." Major grant initiatives within the 2006 Budget include:

- Faster, better-allocated State Homeland Security grants would provide $1 billion for discretionary grants to States and territories. Funds would be awarded to meet national preparedness goals and priorities identified in State homeland security plans. This approach replaces the current State funding formula, which does not target funds for high-risk States or specific needs.
- The Urban Area Security Initiative would provide $1 billion in discretionary grants to urban areas and regions. Funds would be linked to national preparedness goals and specific gaps identified in regional homeland security plans. As in the past, DHS will define eligibility criteria to encourage coordinated planning and avoid duplication. The requested funding level assumes that no more than 50 regions will receive funding, with each required to coordinate their grant applications with surrounding States.
- The Targeted Infrastructure Protection program would provide $600 million in integrated grants, enabling DHS to supplement State, local, and private infrastructure protection efforts, especially for deployment of nuclear and chemical detection capabilities and security investments at ports and other transit facilities. Rather than providing arbitrary amounts for particular sectors, priorities and projects would be determined based on relative risk, vulnerability, and need.
- The Assistance to Firefighters Grants program would provide $500 million in competitive grants to fire departments and emergency medical providers.[39]

In Iowa, Homeland Security funding is administered through the Iowa Homeland Security and Emergency Management Division (HSLEM). To date, the HSLEM has provided a grant of $233,270 to support the creation of the CJIS strategic plan. Information sharing among the criminal justice system is a priority, according to the HSLEM 2005 Homeland Security Strategy. The document includes specific information sharing recommendations for the criminal justice community:

Implement the criminal justice information system across Iowa utilizing a three-step process (2005):

- *Bring together disparate operating systems that were developed independently in the criminal justice arena.*
- *Maximize the use of electronic technology and minimize the use of paper information sharing.*

[39] *InfoLetter*

- *Support the implementation of a criminal justice information system integration project by developing an implementation schedule and identifying federal and other funds that could be used to advance the project.*[40]

The MAXIMUS/URL Integration Team encourages the continued partnership and collaboration between the CJIS Program Office and HSLEM.

5.1.2.4 Federal Earmarks

Each year, through many of the grant programs listed above, the U.S. Congress provides billions of dollars of support to state and local agencies. Most of these grant opportunities are passed down from the federal government to state and local applicants via a method defined by statute, such as the Byrne formula grant program described above. Congress has also created funding opportunities that are discretionary in nature, meaning that the federal agency distributing the funds has the authority (subject to federal rulemaking provisions) to administer grant funding competitively in program areas that the agency deems timely or important to the field.

However, in recent years, congressional appropriators have reduced the amount of discretionary dollars available to federal agencies by earmarking, or setting aside an allocation of funds for a particular person or cause. Earmarking allows the U.S. Congress to direct and control how the discretionary elements of the federal budget are being spent, but limits the ability of the agencies to support field-based initiatives. Examples of these funding streams in an integrated justice environment include the Law Enforcement Information Technology grants funded through the U.S. Department of Justice, Community Oriented Policing Services (COPS) office. This program was funded at $138 million in FY 2005, of which almost all is set aside for specific projects or programs for jurisdictions all around the country.

This trend could present an opportunity for the CJIS Program Office. Part of the CJIS outreach effort to decision makers should include educating members of the Iowa State Congressional delegation.

5.1.2.5 State Revenue Sources to Support CJIS

In addition to the decreasing availability of federal funding to support CJIS efforts, federal funding sources are helpful to support specific projects but infrequently support ongoing operations. State revenue sources – including general fund appropriations – are a far better source of ongoing support for CJIS initiative.

[40] *The Iowa Homeland Security Strategy 2005*, page 24.

In Iowa, there are several state revenue sources that can support the CJIS effort: the Local Government Innovation Fund (LGIF) and the State Return on Investment (SROI) program. To date, the CJIS effort has received $920,414 in funding from SROI,[41] while the LGIF has contributed to the Case Management Project being piloted by the County Attorneys.

According to information released by the State of Iowa Department of Management, the LGIF and its governance Committee were created by the 80th General Assembly to encourage and support innovation at the local level. A $975,000 appropriation was made of which 80% was available for loans and 20% as grant awards. The committee set the interest rate for the five-year term loans with a single annual payment at 2% and opened the first of two application periods in January 2004. The first round drew 70 applications. There were nine applicants awarded funding in the first round, three received both a grant and loan while only one applied for just a loan. First round awards were comprised of $280,000 in grants and $231,000 in loans totaling $511,000.

A legislative change last session eliminated the 80/20 language leaving that determination to the LGIF Committee. The second round accepted applications through July ending August 2, 2004. Only 12 applications were received; seven of those received awards of grants totaling $460,000. Local Government Innovation Fund awards for the two periods totaled $971,000. The fund is essentially exhausted with only $1,800 remaining after deducting committee expenses.[42]

The SROI is a funding source for state-level IT projects, which requires applying agencies to document the expected costs of an IT initiative as well as its expected benefits based on a predetermined set of criteria. According to an article about the program in *CIO Magazine*, the Return on Investment Program Funding Application must be completed for any expenditure over $100,000, Pooled Technology Account requests, any request for money from a source outside of an agency's annual appropriation, and any expenditure that is not routine. Waivers that let agencies skip the ROI process are allowed for some large, routine expenses but are quietly discouraged.

An information technology council—including the Iowa CIO, the CIOs from major state agencies, representatives from the state Judicial and Legislative Branches, and private citizens—scores each application and ranks them. Projects can earn up to 15 points for fulfilling a legal mandate or complying with enterprise technology standards. Improving customer service may garner another 15 points. The bulk of the remaining score takes into account such factors as ROI and risk, whether the project will streamline business processes, whether it affects multiple agencies and, for multiyear projects, the success of earlier phases. The application includes a methodology for assessing benefits that—as is

[41] *CJIS Funding*
[42] Local Government Innovation Fund website at http://www.dom.state.ia.us/innovation_fund/Guidelines_and_App_Process.html

the case with many public-sector initiatives—aren't easily quantifiable[43].

New Revenue Sources and Fees

In many jurisdictions, justice information sharing is supported by fees levied by the criminal justice system against offenders for the services provided through the judicial process. This sort of user fee is typically politically palatable, since the users of the services (offenders) are those who end up bearing the burden of the cost of these fees. According to the *Pre-RFP Toolkit*, a publication of the Integrated Justice Information Systems (IJIS) Institute and the Justice Information Sharing Practitioners (JISP), examples of such fees include:

- Special fees, such as an enhanced 911 fee for both landline and wireless communications, or from additional fees charged to offenders through court proceedings.
- Many agencies charge user fees based on the number of individuals within the participating agency who use the integrated justice system. This approach is particularly effective in funding long-term costs.
- Some states have used either existing fees or increased fees on motor vehicle and boat transactions. Due to the large number of transactions, these fees can generate significant funds.
- Several states have gaming operations that generate significant sums of revenue. Dividing the existing revenue collected or increasing the amount of revenue collected can provide a significant source of funds, both in the short and long term.
- Some state and local governments have adopted specific fees, increased existing fees, or diverted some of the revenues from existing fees to fund new IT initiatives.[44]

There are other options for larger scale, longer term funding. In some jurisdictions, creating a bond issuance is an option to raise a large amount of funding for a new initiative. The bond proceeds are a long-term financing method that can be used for purchases that average 20 years to repay. For instance, a government entity needing $5 million for infrastructure could prepare a public bond issue. The government entity obtains the money right away and makes payments through a debt service.

Revolving funds offer another way of raising funds for IT projects that do not rely solely on the traditional tax levy. Revolving funds allow agencies to establish a revolving fund from which agencies could borrow for IT proposals. Agencies then repay the fund from

[43] *R.O.Iowa*, CIO Magazine, June 1, 2003 at http://www.cio.com/archive/060103/iowa.html?printversion=yes

[44] *Pre-RFP Toolkit*, Integrated Justice Information Systems (IJIS) Institute and Justice Information Sharing Professionals, www.ijis.org.

cost savings or new revenues generated as a result of the project. Fund managers decide which projects merit the risk of a loan. The revolving fund thus functions as internal venture capital, supporting risky and longer-term projects that may be much harder to fund through the traditional budget process. Because agencies repay when projects bear fruit, the fund is perpetuated for future IT investments. A surcharge in the fees often used to fund IT services could also be used to support revolving funds.

Finally, part of the CJIS Program Office outreach initiative should be to build partnerships with the private sector and local corporations, foundations, and other non-governmental interests in Iowa. Partnering builds ownership and can assist in developing long-term support – both financial and political – for an initiative. Partners don't necessarily have to contribute funding. Knowledge, services, equipment, and public relations support are examples of contributions that other partners can make. Chambers of Commerce, for example, may become formal project partners because they want to improve public safety to promote tourism and economic development. Furthermore, some industry groups may be interested in assisting a jurisdiction with an IT project in order to test or further develop a new technology. While there is some risk to the agency in taking this approach, in many cases the firm offers its services to the jurisdiction at a significantly reduced or no cost.

It is important that partnering agreements are formalized in writing so that all parties are clear about project responsibilities, as well as the benefits of participation. Sometimes, when partners are not contributing financially to a project, the project responsibilities can be taken too casually. Drafting a partnership agreement in the form of a Memorandum of Understanding can help create the team discipline necessary to accomplish and further project goals.

5.1.2.6 Recommendations

Overall, we recommend that the CJIS Program Office cast a wide net with regard to seeking funding and support for CJIS initiatives. As pointed out above, some funding sources, such as grants or earmarks may be appropriate for specific projects, while support created through a special fee may be more appropriate for longer-term operational support. Working to cultivate support at these multiple levels will increase the longevity of the CJIS Program Office and its ability to fund specific initiatives in support of justice integration in Iowa.

Specifically, we have the following recommendations regarding funding:

- *Seek general fund appropriations from the Iowa Legislature.* The Years One through Five implementation plan set the funding estimates necessary to support CJIS Implementation in Iowa. The CJIS Advisory Committee should immediately begin working with the legislature to secure funding to begin implementation activities while also shoring funding from other sources. This action is important both in the immediate term but also to create an expectation

among state-level policymakers that CJIS is a program rather than a project, and that continued funding is essential.

- *Create access to federal grants.* The CJIS Program Office should begin working collaboratively with the Iowa ODCP and the Iowa Department of Homeland Security and Emergency Management, to identify how integrated justice fits into the overall state criminal justice and homeland security planning processes.
- *Cultivate support for a longer-term operational funding stream.* Creating a new special fee to support CJIS operational costs will take time to develop. Begin the process of reaching out to key decision makers, such as elected officials and key officials in the Executive Branch, to develop support for a new fee.
- *Consider an earmark.* Congressional earmarks can provide a large infusion of cash for a program such as CJIS, though the funding is typically set aside to support a specific initiative, rather than for long-term operational support. This funding source will take some time to develop, however, and as such, it is good to begin cultivating relationships with elected officials.
- *Develop relationships with the private sector.* Many businesses and private sector organizations are also concerned about the quality of life and safety of the communities in which they do business. Large Iowa-based corporations may be willing to partner with the State to provide cash or in-kind contributions in support of justice information sharing.

5.2 Integration Timeline

This section outlines the recommended implementation timeline for the Iowa Criminal Justice Information System over the next five years. The recommendations are presented by Fiscal Year (FY), and Year One is considered to be FY 2006, beginning July 1, 2005. The MAXIMUS/URL Team understands that is too soon to have received a new general fund appropriation for CJIS, however it is crucial that momentum not be lost waiting a year for new funding. Significant work can be undertaken in the first year, while aggressive, and nevertheless can be done before the significant project costs are incurred.

CJIS planning has already completed an extensive amount of work over the past few years as outlined in the previous sections. As noted, there have been significant strides made, and it is this momentum that needs to be maintained. Although the timeline reflects the current year as Year One, in actuality it may be seen more broadly as entering the first year of the development and implementation phase of CJIS.

The costs that are associated with the implementation timeline will vary as timelines shift in future years. The costs also reflect a high/low estimate as it is difficult to precisely determine specific costs without the State having made decisions based upon recommendations laid out in this plan. The low-end costs often reflect what the MAXIMUS/URL Team believes the State would require to meet the incremental goals of the project; the high-end would meet these goals while mitigating the State's risk by

providing room for unforeseen issues in implementation and a more technically robust environment.

The hardware and software that will make the electronic exchange of information possible both at the agency level and at the CJIS level is intended to facilitate the exchange of information between existing systems and in no way replace their functionality or build a new justice "system." But as CJIS becomes operational, the agencies will depend more and more upon its availability and reliability and will come to expect it to perform at least as equally well as their own. We have accounted for this increase in expectation for availability in the high-end numbers, and while we suggest this is realistic, there is an incremental approach the State may take in bringing on the fully operational environment.

The recommended tasks and timeline are just that – recommendations; they do not presume to imply an all or nothing approach. However, it is important to understand that many tasks are dependent upon other tasks having been completed or begun. In other words, tasks cannot be pulled out individually without there being an effect upon the expected outcomes of the plan as it is written. Some tasks and their ordering are critical; others may be delayed, reordered, or not undertaken at all without having a major impact upon the CJIS project as a whole. There are of course alternatives to the prescribed solutions for a specific goal which may also be substituted without consequence, while other changes may pose a significant enough change to make the plan as written weaker. How the various tasks fall regarding these categories may be readily apparent and for others will require further analysis.

5.2.1 Integration Activities, Milestones, and Deliverables - Year One

Year One of the CJIS project begins upon the acceptance of this plan by the CJIS Advisory Committee. The time of the plan's acceptance is such that it coincides with the beginning of the State's fiscal year. There are assumptions made in setting out tasks for the first year that are dependant upon decisions made by the Advisory Committee after having had the opportunity to fully evaluate the recommendations and their implications. The tasks and timelines recommended for Year One are set at an aggressive pace and are only possible if work begins in late first quarter of the fiscal year.

The tasks are ordered in this text chronologically where possible; however, some tasks are recommended to be performed simultaneously with others, and while they follow in order, it does not necessarily imply chronology or importance.

5.2.1.1 Governance/Project Management

There are several critical initial tasks that should be undertaken immediately to establish a structure for the management and support of the CJIS project. The CJIS project currently has a single full-time employee (FTE) coordinating the effort, which has served the CJIS effort well to this point. However, as the development and implementation of electronic exchanges begins, the role and structure surrounding CJIS will require an

organizational infrastructure. The CJIS Advisory Committee should determine the location of a CJIS Office and recommended staffing throughout the lifecycle of the project. It has been recommended in this plan that the CJIS office be permanently established in Division of Criminal and Juvenile Justice Planning (CJJP) with a coordinator position and three support FTEs. The recommended positions are: a domain/business modeling expert for data and business practice related tasks, a developer for the CJIS message Broker implementing and supporting the electronic exchanges, and a help desk staff person to assist the justice agencies in CJIS related issues. The Office would administratively report to the Director of CJJP and report to the CJIS Advisory Committee for all policy and practice-related matters.

The several recommendations in the plan include TraCS becoming an integral part of the CJIS electronic workflow and conforming TraCS documents and technology to CJIS standards. The Department of Transportation will need to be consulted for this to effectively take place. If agreed-upon, the CJIS MOU will require modification to include the DOT as a part of the CJIS Advisory Committee.

The Department of Administration's Information Technology Enterprise (ITE) has been recommended as the site for housing the CJIS message Broker. The Broker will manage messaging and routing based upon the justice systems business rules. The messaging function of the Broker is dependant upon the specific architecture the justice agencies have agreed to and also must be maintained to strictly enforce the agreed-upon business rules for electronically exchanging justice information. While ITE affords the best option for physically housing the technology, it is recommended that an agreement be reached with ITE whereby the CJIS Advisory Board and CJIS Office oversee the technical standards as well as the development on the Broker. This agreement would include the services ITE would provide as well as where CJIS would remain autonomous from other ITE standards and practices.

To meet the CJIS standards for technology and justice community practice the CJIS technology housed at ITE may require formal (reasonable) exemption from the newly enacted CIO Council standards they may set. CJIS will represent not just Executive Branch agencies but the Judicial Branch and local government requiring flexibility in the arrangement.

5.2.1.2 Legal Issues

The Iowa Constitution requires notary attestation on Criminal Filing Instruments, and thus far the Courts have only accepted a notarized paper document to initiate a criminal filing. In the case of the electronic transfer of traffic citation information to the Court via TraCS, the court does assign a case number upon receipt of the data but will not set up the financials or the court appearance date in ICIS until the clerk has received a paper filing. Even with this staged process, the Court clerk is saved the burden of entering the all of the information from the citation into ICIS. But, the current practice cannot fully benefit law enforcement and the Court clerk until the burdensome handling of the paper

filing is no longer required. The Courts are planning to initiate pilot electronic filing projects in non-criminal proceedings where no such attestation requirement exists. The pilot efforts are expected to begin in 2006 and the optimal situation would be for the approach to electronic filing be consistent across all case types.

Criminal electronic filing is a highly desirable goal of CJIS. If it is to be achieved in the near term, the legal issues and possible mechanisms to ensure the intent of the constitution is met while taking advantage of current electronically equivalent assurance methods, such as public key infrastructure security technologies, is necessary. The MAXIMUS/URL Team recommends that a business process review is undertaken, to identify any business process changes necessary in accepting digital signatures and ensuring compliance with the Atsinger decision and the need for independent verification of criminal complaints. Determining what can be done through Iowa Administrative Code, Iowa Court Rule regarding issues before Iowa Code change or any constitutional amendment are considered should be done prior to putting together the legislative package for Year Two.

5.2.1.3 Policy Issues

There are several policy issues relating to integrated justice that were identified as barriers in this plan. It is recommended these policy issues be addressed in Year One. There is no need to delay addressing identified policy issues, as they have been perceived as difficult issues to resolve and there is no reason to believe they will become easier as time passes.

A significant policy area that will need to be addressed involves the relationship to local criminal justice workflow and the policies of the state agencies, and whether the justice workflow can take advantage of the strong State systems to disseminate information to other local agencies or even to each other. Traditionally, the State agencies have served their stakeholders, such as the Department of Public Safety serving policing agencies and the State Court Administrator's Office serving the Courts. In an integrated environment, the lines will become blurred and policies that once served to enhance the data integrity may in fact become detractors. Trusted relationships will need to be established between the State agencies that allow flexibility while at the same time protect the highly valued data each agency is responsible for maintaining.

Policy questions will need to be answered such that new business approaches that on the surface challenge old practices are seen from a broader criminal justice perspective. This allows change on both sides of an information sharing exchange to take place. Specific examples of this include the ability to query information on the IOWA System without being logged into the IOWA System, instituting some form of secondary review for sensitive information being entered by external agencies into the IOWA System, and standardizing on statewide person and incident/case identifiers.

These issues do not need to be resolved before work can begin on other tasks, but the longer they are delayed the longer it will be before the benefits of integration can be fully realized in the business practice of justice in Iowa. The impact of non-decisions will be realized when the exchanges and related processes are being designed and implemented.

5.2.1.4 Legislative Package

A legislative package must be the first major deliverable in Year One of the CJIS project, and then become an annual task. The recommendations made by the MAXIMUS/URL Team should be finalized through the CJIS Advisory Committee and submitted to the Legislature as a part of a complete request package. The "legislative package" would include the finalized plan, the funding request with a timeline for the specific exchanges to be implemented, and any proposed CJIS related Iowa Code changes.

This plan recommends each year's fiscal request be based not only upon the merits of the request but the demonstrated gains of the previous year. This requires the package of information submitted to not only include what is to be accomplished with proposed FY appropriation for the following year but a way to measure the accomplishments. The section of the plan that describes performance measures will assist in this measurement. It also implies that work done this year is documented in the submission.

5.2.1.5 Exchanges

Each year will have business processes and specific exchanges targeted for design, development, and implementation. Year One will begin this process using existing exchanges as "Proof of Concept" for the new process, architecture and direction. Three exchanges will be undertaken during the first year to put in place a level of functionality for data exchanges in the service-oriented environment. It is intended that these exchanges be implemented prior to the implementation of the CJIS Broker. These will be the Uniform Traffic Citation and Complaint from local law enforcement agencies to the Courts, the Protective Order from the Courts to the IOWA System and the Pre-Sentence Investigation (PSI) between the Courts and Corrections.

For selected exchanges, an Information Exchange Package Description (IEPD) will need to be developed. It is through this process that the data standards for each document exchanged are defined based upon GJXDM conformance. The data model, schema, document layout, and distinct data requirements are described. The IEPD development process will involve practitioners from agencies using the document and facilitated by CJIS Office staff. Use cases will also need to be defined for each endpoint in the exchange. The use case will identify how each agency sending and receiving interact internally with the exchange from a business function perspective. It is at this point that issues such as real-time data entry and consistent practices are identified and addressed.

Each agency application participating in an automated exchange is triggered by a business event that must be examined to find the triggering mechanism to send or receive information. Most applications were not designed for interaction with an automated triggering mechanism but with a human entering or querying through a screen. Before the applications can begin to exchange data with another system's application, they must be aware of the need to exchange information.

They major project efforts for DPS, Judicial Branch, DOC, and DOT (TraCS) based upon the exchanges are broken down as follows:

- **Data Standards Development** – This task will initiate in Year One and continue through Year Five. Initially, this will be through the development of IEPDs, an inventory of the GJXDM model to ascertain elements relevant to Iowa data exchanges and then elements specific to Iowa will be defined and created, ultimately arriving at an extension namespace specific to Iowa and conformant to the GJXDM model.

- **Transaction Processing Analysis** – This project will need to be undertaken by all participant systems to identify, from the perspective of a workflow, what functional areas of their system will result in discrete web services. These functional areas will be considered trigger events that either initiate an exchange or initiate a system process as the result of being the recipient of an exchange.

- **Web Services Implementation** – This task is critical as to implement the service-oriented architecture, it will be necessary for every participant system to have the ability to create or consume a service-oriented access protocol (SOAP) message. This may require in most cases an adapter layer in place to allow the application to interact as a web service. This project will also entail the design and development of the web services themselves in support of transactions taken on during Year One.

- **Network Security** – This task involves two efforts. The first is the selection and implementation of a dual-mode, challenge/response authentication product to support remote users requiring secured connections. The second is to implement new or configure existing firewalls between the middle tier layers in support of automatic secured connections between devices without the need for user supplied credentials.

5.2.1.6 Data Standards

The data standards project will commence during the first year and continue throughout the entire five-year plan. It is important to begin this work right away so as to provide a foundation for all data exchanges. If this work is not done initially and applied to the first transactions implemented during Year One, little value will be gained as a true service-

oriented environment will not be put in place up front. We recommend establishing a Data Standards Working Group to undertake these tasks.

As recommended in the "To-Be" section of the plan, all data exchanges will be implemented as documents structured to an Iowa-specific implementation of the GJXDM model. Consequently, an inventory of the GJXDM model must take place so as to fully ascertain what portions will be relevant to Iowa integration efforts and what will not. This should be accomplished by progressing into defining the IEPDs for the Year One transactions to determine what elements may be required for Iowa that are not in the GJXDM. By progressing through the IEPDs in Years One through Five for all defined exchanges, all extensions should be identified and a comprehensive Iowa-specific namespace arrived at that can be considered GJXDM-conformant. As presented above, the Uniform Traffic Citation and Complaint data exchange, Pre-Sentence Investigation (PSI), and Protective Order will be implemented during year one.

It will be necessary for the Data Standards Working Group to accurately define a comprehensive IEPD for the Uniform Traffic Citation and Complaint document – one that defines not just criminal and traffic citations, but accounts for similar charging documents as well. In short, this document must present a structured set of allowable fields for all specific documents that will be the actual transmissions in the data exchange (request and response in same IEPD). The same effort must be done to build an IEPD for the PSI and Protective Order exchanges.

During the first year, it will be important to launch the data standards effort successfully such that all subsequent data standards efforts can map back to the same comprehensive namespace for Iowa as well as reuse data structures previously defined.

While only the Uniform Traffic Citation and Complaint, the PSI, and the Protective Order are recommended as first year POC implementations, it is also recommended the data standards committee begins IEPD work only on the following in Year One:

- Complaint and Affidavit (Preliminary Complaint)
- Trial Information
- Warrant
- Incident Report

.

Outcomes from this effort will be the individual IEPDs but also the first version of an Iowa justice domain data model based on the GJXDM and local Iowa extensions. The model will include the documents and reusable components that should be used in the development of subsequent documents. In other words, the model itself and its components should not be directly dependent on upon the GJXDM but should instead map to and extend the GJXDM to be Iowa-specific. It is the mapping that will be tightly coupled with the GJXDM and could, as a result, be impacted by new releases.

The GJXDM and other models used by the federal government, such as the National Information Exchange Model (NIEM), are currently in the conceptual phase and will likely change based on the needs of large constituent communities. The MAXIMUS/URL Team is not recommending that each IEPD developed to continually change to keep pace with the GJXDM or other models; rather it is our recommendation that the evolving Iowa domain model should change based upon the business needs of the Iowa justice community. While there may be a need to adopt changes based upon exchanges with entities outside of the State of Iowa or as required by federal grant making agencies, changes in the GJXDM release should not affect the majority IEPDs developed for in-state use.

The Iowa domain data model and subsequent IEPDs may also map to distinct versions of the GJXDM depending on when they were developed and the cost/benefit ratio of bringing existing IEPDs up to new GJXDM release conformity. There will be a cost to maintaining the Iowa IEPDs conformance with the latest GJXDM version, and this should be evaluated on a document by document basis.

The GJXDM versions are numbered by three integers X, Y, and Z delimited by periods:

Syntax: X.Y.Z

Each integer represents a particular class of change:

- X = Major revisions to the model or representations of the model as rendered in a schema (as XML or other markup)
- Y = Minor changes that do not maintain forward compatibility
- Z = Minor changes that maintain forward compatibility

At the time of this report, the GJXDM is at version 3.0.2, with 3.0.3 soon to be released. The Justice Department expects that release 3.1 will be out within the next six months.

A "..Z" release will fix bugs, introduce new elements, and deprecate a number of elements. Elements are deprecated to warn users of their pending deletion in future releases. The "..Z" release maintains forward compatibility, meaning the new "..Z" release of the GJXDM would be fully compatible with IEPDs developed using the previous "..Z" version. Items deprecated, while they are still available in the next release, should not be used for new development.

A ".Y." release will introduce potentially structural changes that will not maintain forward compatibility with previous releases of the GJXDM. However, any one IEPD may not be affected as the changes were to parts of the model not used in the IEPDs subset schema.[45]

[45] Source http://it.ojp.gov/jxdm/faq.html "Global Justice XML Data Model Frequently Asked Questions."

An "X.." release will, by definition, introduce significant changes that could permeate across the entire model affecting all schemas developed under previous versions.

Iowa will need to follow the progress of the GJXDM regularly, particularly as major releases are announced. However, it is anticipated the future major changes will only enhance the reusability of components within the current GJXDM.

5.2.1.7 Transaction Processing Analysis

During the first year, the Transaction Processing Analysis task and the POC Web Services Implementation tasks will come together. The Transaction Processing Analysis project will need to occur first, and in short, is an analysis of each participating system's business processes to arrive at a Use Case of how and where tasks are accomplished. The goal of this effort is to identify specific points within the workflow where data exchanges are initiated or where a data exchange is received, initiating a process within the workflow. This bidirectional analysis will be key in determining the trigger events within the system that not only send a transaction but also what system processes are initiated by the receipt of a transaction. Essentially this will be a mapping of the specific system modules for an application to the previously defined data exchanges, exposing where they already fit and where gaps may be present.

This effort will necessarily begin with an analysis of the existing business processes and their corresponding parts of the system. Business analysts will examine the systems flow up front, and then systems analysts will identify sections of the application code where the trigger events will occur.

This effort may already be well understood for each system and in those cases the analysis effort is likely to not be significant. But regardless of how straightforward this work is for a given system, it will be important to lay out the defined trigger events within the context of a workflow so as to provide an inventory of functionality that will be encapsulated as services within the proposed web services layer. Additionally, the workflow analysis results from all participant systems will drive the necessary business logic that needs to be part of the centralized Broker system design and implementation during the second year.

The major deliverable from this task will be a document that identifies the trigger events of a given system within the context of that application's workflows in use case, activity, and sequence diagrams. It should also provide specifications for the areas of functionality within the application code that already exist modularly or need to be structured so that they are discrete modules. Additionally, the expectations for the type of message or "payload" sent or received should be specified. These trigger events and their corresponding functionality will be the source for the implementations of specific web services and help define their role as push/pull/query-oriented services.

5.2.1.8 Web Services Implementation

The Transaction Processing Analysis project will produce for each participant system a set of trigger events that need to have their functionality captured and abstracted into an application web services layer. This most likely will require the acquisition or development of adapters to expose the functionality of the application to the web services layer. The goal is to accomplish this while preserving the original application and its full functionality as much as possible. Service adapters expose application services to Broker or other services while event adapters publish asynchronous, unsolicited messages from the application to external services or the message Broker. Adapters can be developed through Broker vendor-provided Adapter Development Kits, purchased through adapter framework vendors, or custom developed through open APIs if the agency environment supports this functionality.

Trigger events that initiate a data exchange (or transaction) will build and package the message to send it to the recipient system. Those trigger events that are identified as active only upon receipt of an exchange will be serviced by listening services that take an incoming transaction and pass the message along to the system for process. Both types of services will need to be in place to support the end-to-end functionality of the data exchanges across the five years. During Year One, the focus will be on constructing the services necessary to support the initial transactions described above. To accomplish this, it will first be necessary to establish this layer for each participant system.

ICIS (especially ICIS2) and ICON already have robust application server layers capable of supporting web services. ICIS2 applications will have the ability to directly interface with web service layers without the need for adapters. The TraCS Office implementations and other RMS systems used by local law enforcement agencies do not necessarily provide a physically or logically separate application server layer that can be easily configured for a web service environment. It is recommended that as part of this project, a centralized middle tier (TraCS Broker) layer to support web services for all local law enforcement agencies be developed and implemented at DPS.

DOT has expressed intentions to fully implement the recommendations in the ECCO Audit conducted by Cisco. This plan anticipates the proposed TraCS Broker located at DPS to provide the services CJIS requires to move Citations to the Courts and eventually dispositions back to DOT and LEA. Any expected cost or timelines for this effort have not been published at the time of this writing. It is critical that at least one jurisdiction has the ability through TraCS to pass a SOAP message to DPS for the Traffic Citation POC. During the first year, in support of the automated transfer of complaint/citation exchanges between the local law enforcement agencies and ICIS, services will necessarily be constructed in this new centralized middle tier at DPS as well as ICIS in support of this exchange.

The proposed Protective Order Exchange between ICIS and the Iowa System would require the IOWA System to expose the protective order application to a web service

layer. None of the current functionality would be compromised; however, the application would receive a SOAP message with an XML payload directly from ICIS. The ICIS No Contact application already triggers an exchange; however, the application would now be required to build and send a SOAP message corresponding to the listening service on DPS. This exchange would be bi-directional with DPS sending ICIS back the result of the exchange.

For ICIS and ICON, these systems would utilize their results from their respective Transaction Processing Analyses to identify what pieces of functionality to build as web services. During Year One, services to support the data exchanges of PSI orders between ICIS and ICON will be constructed. This would require services on the ICIS side to build and send the PSI order request and a corresponding listening service on the ICON side to receive or "consume" this request. Upon completion of a PSI order by DOC, a service on the ICON side would build and send the message containing the completed PSI order back to ICIS where it would be picked up by a corresponding listening service.

There are important outcomes from this project: The first is the implementation of a web services middle tier layer for each participant application. This will be tailored to the individual systems that already have a robust application layer and consolidated into a shared middle tier layer at DPS for local law enforcement entities. The second outcome is the design and development of discrete web services based upon the trigger events defined in the Transaction Processing Analysis project. It will be important to maintain open SOAP standards in the development of these services to provide a common messaging format across the integrated environment. Proprietary web service standards cannot be utilized.

5.2.1.9 Network Security

During Year One activities, it will be necessary to initiate the "To-Be" recommendations of implementing secured, encrypted transactions. This covers implementing an authentication solution for remote users and the implementation of firewalls for each participant's middle tier layer.

At this point, no remote connections (i.e., connections originating outside of the State network) are expected to be in place for integration. However, it will be important to select a solution for VPN authentication that augments usernam2e/password upfront. A dual-mode/challenge-response solution (i.e., token card) is recommended, and efforts need to begin in evaluating and selecting a product during this first year.

With respect to firewalls, part of the recommendation for network security described an environment where individual participant systems would put a firewall in place between themselves (i.e., the middle tier web services layer) and the centralized Broker system. The centralized Broker system will not be implemented in Year One, however, the firewall implementation should be done initially, especially for those systems that will be participating in the initial exchanges of Uniform Traffic Citation and Complaint, PSI, and

Protective Order. Existing firewall implementations should be leveraged where possible– a notable example being the ICON system, where firewalls in addition to those provided by the ICN are already in place. The main purposes of the firewall setup are to protect the middle ware layer traffic during integration and enable encrypted VPN connections between devices automatically. Since these systems are within the State network and these data exchanges are automated processes as part of an identified workflow, it is not necessary to have user-supplied credentials to establish the VPN connection.

Outcomes of this project are to have in place a solution for remote authentication whereby participants requiring such connectivity can be brought in as a matter of procedure. Firewall configuration and/or implementation should be in place in Year One for those participants utilizing transactions implemented in this initial phase. Additionally, an action plan for setting all secured network connectivity in place should be created so that early into Year Two, the entire enterprise can be ready to support secured connections with the centralized Broker system.

5.2.1.10 RFP for Message Broker Software/Hardware

A request for proposals (RFP) should be developed prior the end of Year One anticipating the availability of funding. If funding has become available at the beginning of Year Two, the State will be in a position to quickly release the RFP. If funding is not fully available the RFP will then require modification.

Several of the tasks outlined in Year One will require the expenditure of funds mostly from agency existing base resources. However, others will require additional funding, if available, to assist the CJIS office in IEPD development. The web services software recommended for use in the POC exchanges is open standards-based software that is available at no cost. These will eventually be brought into the Broker architecture in Year Two. The adapter software, if purchased, will have an associated cost. As this is a POC, limited trial licenses are usually available and advisable. These efforts should provide valuable information in the development of the RFP for the full Broker solution and what adapters the agencies will require.

5.2.2 Integration Activities, Milestones, and Deliverables - Year Two

5.2.2.1 General Funding

It is anticipated CJIS will receive general funding for the tasks associated with Year Two in July of 2006. At this time, the CJIS office will have the authority to hire the three FTE to support the tasks and ongoing CJIS operation, purchase the recommended hardware and software, CJIS application development, and enter into the contractual relationship with ITE. It is also anticipated that there will be funding allocated to the other state justice agencies specifically directed to CJIS related tasks. Other sources of funding may also be available to support the Year Two tasks.

5.2.2.2 Procurement and Implementation

If the RFP has been prepared in Year One and the funding is available, the process to purchase the message Broker and business flow orchestration hardware and software should occur as soon as possible. There may be adjustments to the RFP based upon funding decisions; nevertheless, this task should be a high priority. In Year Two, installation, development, and implementation will begin on the message Broker, however, this will be with a limited number of exchanges. It is not necessary to purchase licenses and hardware beyond what will be used during Year Two. These can be added on to in subsequent years as the number of exchanges and use of the Broker increases. This would include failover systems as they can also be ratcheted up as the complexity increases.

The County Attorney CMS plan anticipated addressing the web service layer in the second phase of their project. This layer should be procured and added during Year Two allowing the participating County Attorneys to send and receive electronic exchanges. This would also be the case for procuring or developing web service capability for RMS/JMS systems. The CJIS Advisory Committee will be required to make decisions as to which law enforcement agencies and Sheriff offices are in a position to adapt their applications to web services, prioritize the agencies, and recommend the best method to achieve the functionality. The RMS/JMS systems will not all be alike in their ability to adapt to web services. Some RMS/JMS vendors may have this layer available while others may require the development of the web service layer from scratch. In any event, the RMS/JMS systems will be required to use the IEPDs developed for Complaints and Incident Reports so that they meet all the standards a TraCS exchange would appear to the Broker to be the exact same type of exchange.

It is also anticipated that in Year Two DOT will have purchased and developed the method for creating SOAP messages for TraCS exchanges and a persistent storage mechanism for TraCS XML documents. The IEPDs and SOAP messages will be required to conform to CJIS standards. Also with regard to TraCS, the shared middle tier layer or Broker will provide the necessary web services layer in support of the local RMS systems. It will be made up of services that would poll the TraCS office systems at regular intervals to query their databases for information indicating the need to build a document and then create the structured document in preparation for submitting on to the recipient system. In support of local RMS systems robust enough to construct a structured, web service-ready document up front, the centralized services layer would provide for listening services that would route the transaction to the recipient system upon receipt. During Year Two, this centralized services layer would route these transaction from the local law enforcement agencies to the centralized Broker exclusively.

There will also need to be acquired a web user interface (UI) application for County Attorneys to access the charging documents stored persistently at DPS (initially all generated through TraCS). This web UI application would allow County Attorneys to

review charging documents and have the ability to transmit their charging decision to the court. Should the attestation issue be resolved, the exchange could be an e-filing. This application would initially only expose Uniform Traffic Citations but as other charging documents are exchanged would allow for action on these as well. For County Attorneys with the standard CMS, the exchanges would take place through their CMS.

5.2.2.3 Exchanges

The three exchanges developed for the POC Uniform Traffic Citation and Compliant, Protective Order, and PSI will be redirected through the message Broker. This will allow the message Broker technology to be tested on proven exchanges. It will also allow the added benefits of the Broker to be brought to bear on these three critical exchanges.

Once the POC exchanges are moving through the Broker, the exchange IEPDs that were developed for the previous year can begin development and implementation. These business process exchanges include the Complaint and Affidavit (Preliminary Complaint), the Trial Information, the Warrant, and the Incident Report.

The Complaint, Affidavit, and Incident Report could be generated and the message sent out either through TraCS or a RMS, depending on the readiness of the RMS. The Complaint and Affidavit would have the option of being sent to the County Attorney first prior to being sent to the Court. This functionality could either be achieved through a web UI discussed above or the County Attorney CMS.

The same would be true for the Trial Information, depending on the readiness of the County Attorney CMS to either receive or send web service messages. The web UI into charging documents would be the alternative available until they have the functionality or for County Attorneys where the CMS may not be adopted.

The warrant exchange will build off of the lessons learned in the Protective Order POC exchange and the policy resolutions accomplished in Year One. Warrants will require more robust information coming into the Courts from law enforcement and County Attorneys allowing ICIS to contain the information necessary to produce a warrant for posting on the IOWA system. The IEPDs developed for the charging documents will include the paper representation of the new document and this should be implemented even before the electronic transfer so that the Courts are receiving complete data as soon as possible. The Sheriff will receive the broadcast of the warrant similar to how the Protective Order is broadcast currently allowing for enhancement of the record.

Work on OWI Continuum exchanges and the Sentence Orders to DOC and Jails should begin in Year Two by developing those IEPDs. Also, the exchanges between DPS, DOC, and the Judicial Branch to update CJIN, Kaleidoscope, and the JDW will need to be examined. Reuse of IEPD domain models and schemas are encouraged. A key design issue that will need to be resolved is that there are two potential methods taking advantage of real-time, service-oriented, transactional exchanges to meet the business

needs of the justice practitioners. ICON, ICIS, and the DPS (Iowa System, CCH, etc.) could update the data warehouses as an event occurs in their application (e.g., when a offender status change is entered into ICON, it will create a message which the Broker will route to update both Kaleidoscope, CJIN, and the JDW). The other option is based on the fact that DOC has the offender and is not known to Kaleidoscope or CJIN and when an inquiry is performed, it requests the information from ICON at that time in a request/reply set of services. Neither Kaleidoscope nor CJIN will maintain the information permanently. This could be true for CCH information on CJIN, which is now at least a day old.

The Justice Data Warehouse would most likely utilize the first method for continual updates.

Depending on the progress of the initial exchange implementations, the exchanges described above could begin implementation in Year Two.

5.2.3 Integration Activities, Milestones, and Deliverables - Year Three

5.2.3.1 Procurement and Development

The Broker hardware and software license will need to be expanded and the other state agencies' applications web service enabled. The agencies would include the Public Defender's Office, the DOT non-TraCS exchanges, and the Attorney General's Office.

There would be a continuation of the rollout of County Attorney CMS. After Year Two, new rollouts of County Attorney CMS should have the web service layer in place. Web service layers for RMS/JMS systems will continue be put in place based upon the decisions and capabilities determined in Year Two.

As the web service layers are added to local agencies, exchanges that have been implemented previously will have the new jurisdiction added through the Broker.

5.2.3.2 Exchanges

For Years Three and Four the tasks will be building off of the base built in Years One and Two, continuing to rollout exchanges not completed in the previous year and adding new exchanges. Year Three will begin looking at the entire processes required to meet a business goal instead of the single bi-directional exchanges implemented in the first two years. The processes have been outlined in the URL Adult and Juvenile Exchange Reports and these documents should be referenced for further clarification and decision-making.

Rolling out the exchanges begun in Year Two and evaluating the lessons learned will be an initial task of Year Three. Implementing the exchange of the Incident Report from Law Enforcement to the County Attorneys and to DPS for NIBRS (N-DEX) reporting should begin in Year Three. Along with the design, development, and implementation of the following business processes.

- No Contact Order Process
- Publish/Subscribe Type Notifications
- Hearing Court Orders, Notice of Court Date
- Expungement
- Detention (e.g., Release, Bond Order)

These processes will involve a number of individual bi-directional exchanges that have complex business rules. This will need to be taken into account when producing the detailed costs for Years Three through Five.

5.2.4 Integration Activities, Milestones, and Deliverables - Year Four

5.2.4.1 Procurement and Development

As in Year Three, there would be a continuation of the rollout of County Attorney CMS and after Year Two, new rollouts of County Attorney CMS should have the web service layer in place. Web service layers for RMS/JMS systems will continue be put in place based upon the decisions and capabilities determined in Year Two.

As the web service layers are added to local agencies, exchanges that have been implemented previously will have the new jurisdiction added through the Broker.

5.2.4.2 Exchanges

Exchanges begun in Year Three will continue as well as the additional exchange processes beginning design, development, and implementation in Year Four:

- Appellate Process
- Juvenile Formal Adjudication Process
- Motions
- Supervision
- Pre-Trial Supervision

5.2.5 Integration Activities, Milestones, and Deliverables - Year Five

5.2.5.1 Procurement and Development

As in Year Four, there would be a continuation of the rollout of County Attorney Case Management Systems. After Year Two, new rollouts of County Attorney CMS should have the web service layer in place. Web service layers for RMS/JMS systems will continue be put in place based upon the decisions and capabilities determined in Year Two.

As the web service layers are added to local agencies, exchanges that have been implemented previously will have the new jurisdiction added through the Broker.

5.2.5.2 Exchanges

Exchanges begun in Year Three will continue as well as the additional exchange processes beginning design, development, and implementation in Year Four:

- Diversion
- Juvenile Informal Adjudication

5.3 Integration Plan Cost

The Integration Plan Cost section outlines the one-time implementation costs, the recurring operational expenditures, and the spending rates for both categories over the five-year CJIS Integration Plan. The costs presented are intended to provide the CJIS Board, CJIS Advisory Committee, and Iowa CJIS Program Office pricing information to assist in planning and budgeting for achieving the CJIS initiative.

The pricing presented is a cost range based upon known industry items in the category of cost being portrayed in each section and provides a low-end solution versus high-end solution implementation. The labels of "low" and "high" are not intended to denote a superior solution; rather, they are referring to the cost of the category. Typically, the high-end cost adds additional performance for the category denoted, and in this model our high-end pricing reflects what would produce maximum performance. However, we encourage that the specific requirements for performance in the Iowa CJIS Solution be driven by the detailed requirements. The goal of the five-year Integration plan is to implement the best solution for Iowa, which may not be the most expensive solution. The prices are based upon current item costs; however, there is no recommendation being made for the selection of a particular brand item.

The exact implementation costs will only be known as more detailed information about the cost category is determined in the later phases of the plan. The To-Be CJIS Solution presented earlier can be achieved with many combinations of tool, hardware, software, and labor components. The solution dimensions such as processing speed, expected availability, scalability, buying versus building the solution, etc., will need to be assessed in a requirements analysis phase to determine the exact configuration and costs that will be necessary to implement the solution. The low-end and high-end architectures are presented as separate diagrams. The intent is to show what each architecture would look like once fully implemented by the end of the five-year period. It is possible to envision an architecture where some components are not implemented initially (e.g., XML accelerators or full failover capacity implemented as clustered server solutions).

5.3.1 Implementation Cost

The implementation costs are those one-time occurring expenditures that will be necessary for the implementation of the CJIS Broker. Implementation includes the categories of hardware procurement, software procurement, and solution implementation.

Each category presents a low-end versus high-end scenario, but does not infer that one solution is superior to the other. The particular expenditure for the categories will be based upon several factors to be determined during the five-year CJIS Integration Plan execution. These factors will determine what the best solution is for Iowa. Factors that need to be considered in the final cost scenario are:

- Detailed system functional requirements
- Detailed system non-functional requirements
- Iowa CJIS policies
- Iowa CJIS technology standards
- Available funding

The particulars of these factors are just beginning to emerge, and should be considered more fully in the initial stages of the five-year Plan to ensure detailed costing scenarios can be created to drive the funding efforts of the CJIS Program Office.

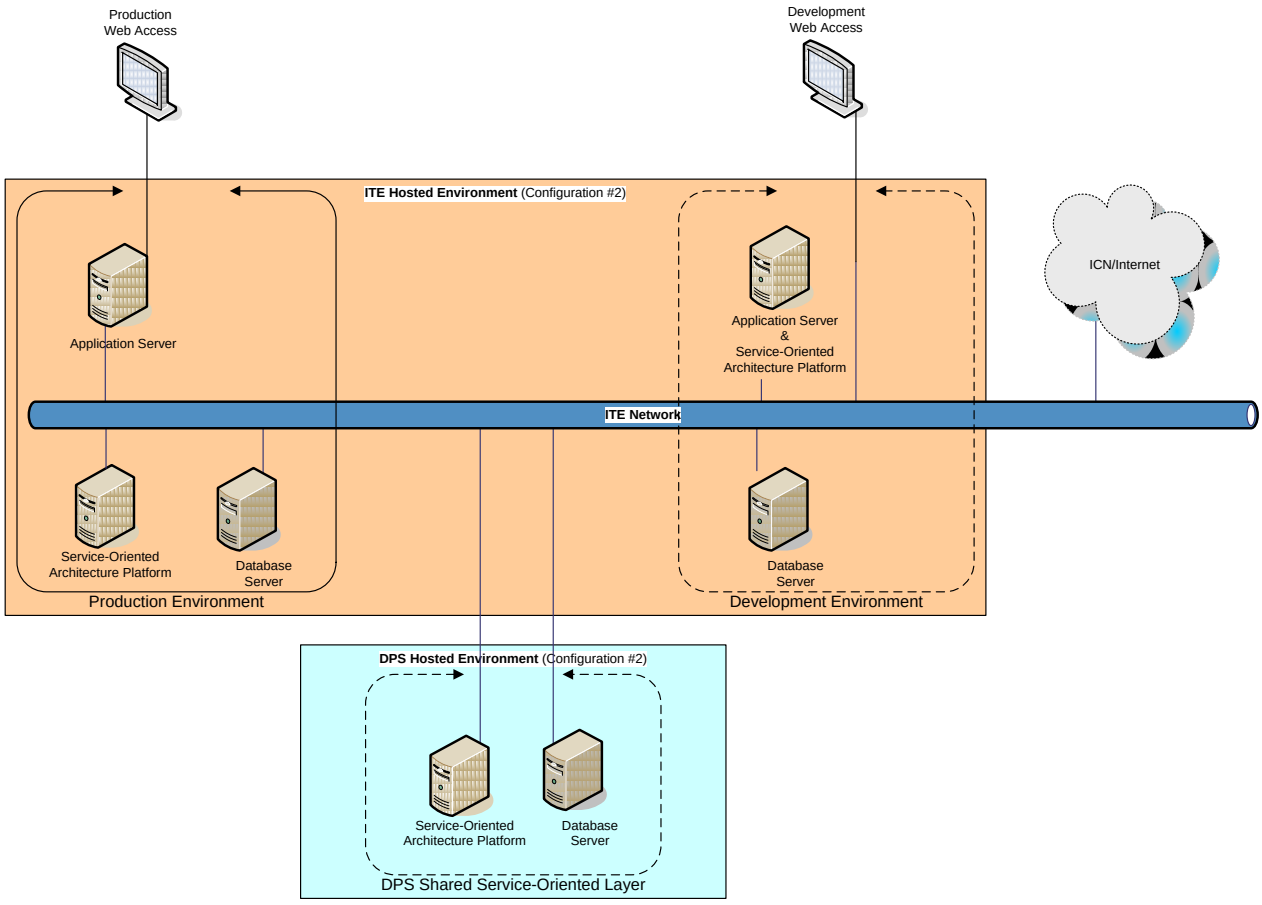
Also, it is important to note that there is not a pure buy/cost scenario for the CJIS Broker being presented. While there are several COTS solutions that provide portions of the functionality necessary for achieving the Iowa CJIS initiative, there is not a single solution for all the functionality known at this time. Even if the State determines that buying particular components of the system as COTS items, integration of those components into a single solution will require some software development life-cycle activity.

5.3.1.1 CJIS Broker Hardware Costs

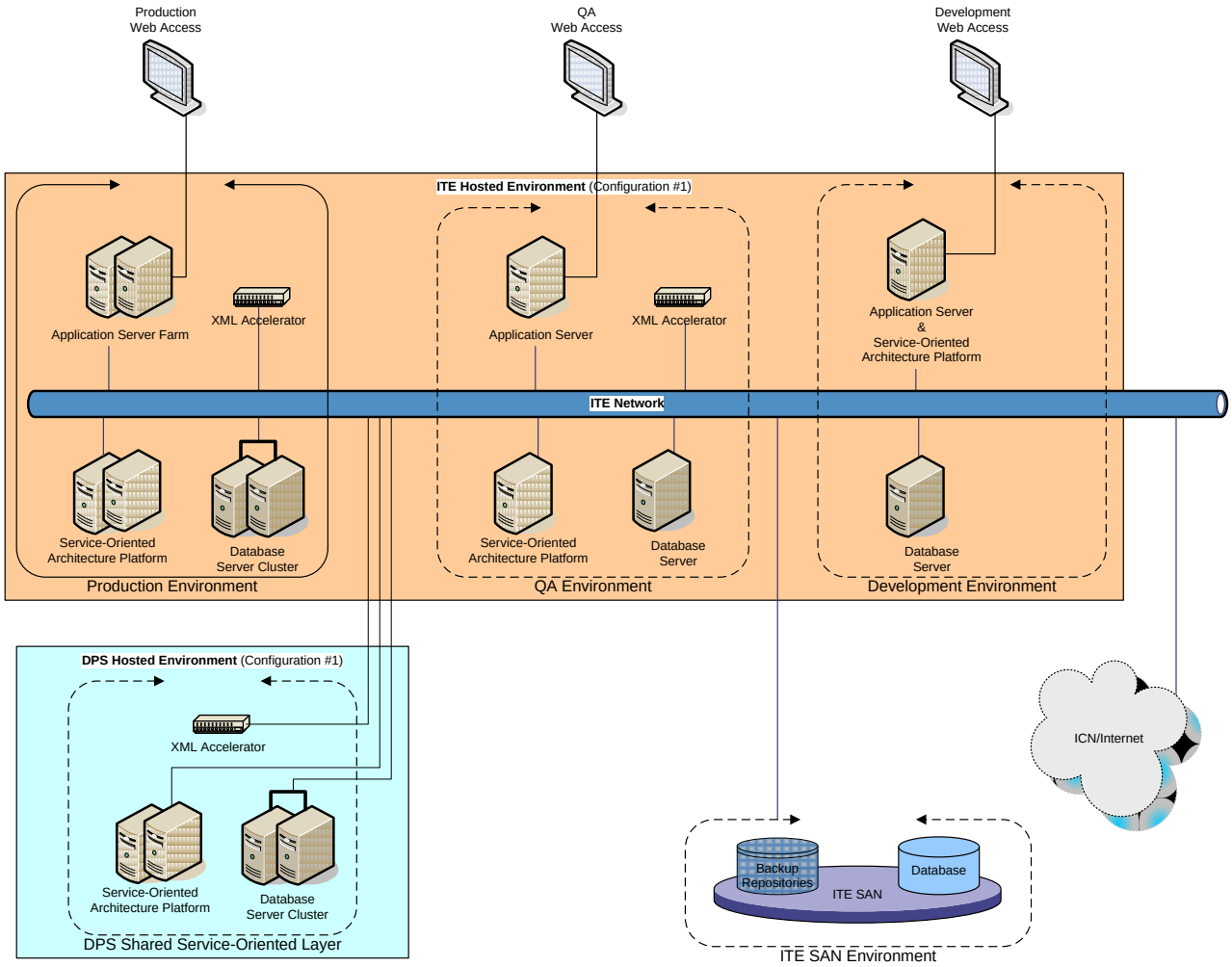
This section covers all hardware costs associated with the CJIS Broker solution. This includes items such as Application Servers, Database Servers, and advanced networking/acceleration devices. Each hardware item listed will show details for the high-end versus low-end option.

The following two exhibits illustrate the CJIS Broker hardware infrastructure for the high-end and the low-end options along side the ITE Network and ITE SAN Environment. Both exhibits are logical representations of the proposed technical environments and depict the physical servers that will make up the CJIS Broker in two separate physical environments. The DPS shared Service-Oriented Layer is the region that will be the first proof of concept for the CJIS Integration Plan. This physical region will support the broker of the initial exchanges selected in the first fiscal year of the plan acting as a gateway for both the TraCS and RMS systems. The ITE Hosted Environment depicts the physical servers necessary for the expanded and fully function CJIS Broker described in the To-be Technical Environment. The following sections describe the components within the technical infrastructure.

The low-end option for the CJIS Broker technical infrastructure is presented below.



The high-end option for the CJIS Broker technical infrastructure is presented below.



5.3.1.1.1 Application Server

The Application Server is the physical server that provides the core User Interface (UI) to the CJIS Broker. In the low-end solution this is a single server, and in the high-end an Application Server Farm is proposed. This Application Server provides the front-end application necessary to provide a technical solution where no automated solutions exists such as the County Attorney's requiring e-filing without Case Management Systems, as well as the UI components for more mature functionality such as subscription and notification services.

The following table depicts the low-end units and cost as well as the high-end units and cost for the Application Server.

Description	Low-End Option			High-End Option		
	Units Required	Unit Cost	Total	Units Required	Unit Cost	Total
Application Server	1	$9,098.72	$9,098.72	3	$19,995.00	$59,985.00

5.3.1.1.2 XML Accelerator

The XML Accelerator Server is a hardware device used to increase performance of XML-related processing and communications in the CJIS Broker. The XML Accelerator is a hardware accelerator – meaning the device offloads existing XML processing functionality from any device onto the XML Accelerator. As such, the XML Accelerator is an optional device in the CJIS Broker – depending on the XML processing load and desired performance needs of the State. Costing for the XML Accelerator has been included in the high-end configuration, but it should be noted that the low-end configuration could also utilize this component if the processing requirement of the final implementation determine it is applicable. The cost range for both the low- and high-end configuration is identical.

The following table depicts the low-end units and cost as well as the high-end units and cost for the XML Accelerator Server.

Description	Low-End Option			High-End Option		
	Units Required	Unit Cost	Total	Units Required	Unit Cost	Total
XML Accelerator	0	$35,000.00	0.00	3	$35,000.00	$105,000.00

5.3.1.1.3 Service-Oriented Architecture Platform

The Service-Oriented Architecture Platform Server is the business processing server that provides advanced business rule processing for the CJIS Broker. These physical servers functions as the core business intelligence engine of the CJIS Broker, processing business rules and providing the essential corridors to CJIS Broker data stores. The Development Environments of both of the proposed configurations utilizes the same physical server as the environment to house the Application Server environments as well. In the high-end solution the configuration supports a redundant, highly available deployment that would be recommended for a mission critical 24X7 system. The determination for this type of procurement would be determined by the required "up" time for the system during the requirements definition of the application.

The following table depicts the low-end units and cost as well as the high-end units and cost for the Service-Oriented Architecture Platform.

	Low-End Option			High-End Option		
Description	**Units Required**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
SOA Platform Server	3	$9,098.72	$27,296.16	6	$19,995.00	$119,970.00

5.3.1.1.4 Database Server

The Database Server provides the data storage and retention functionality for the CJIS Broker as well as CJIS related data. The CJIS Broker's configuration, processing, and queue data is maintained via the Database Server as well as CJIS data. The high-end configuration provides for data redundancy and high availability not being deployed in the low-end configuration.

The following table depicts the low-end units and cost as well as the high-end units and cost for the Database Server.

	Low-End Option			High-End Option		
Description	**Units Required**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
Database Server	3	$33,027.39	$99,082.17	6	$56,938.95	$341,633.70

The Database Servers contain the Database software, however it should be noted that the data files (e.g., physical files CJIS Broker data resides in) will be located on the storage area network (SAN) and not on the Database Server in the high-end configuration.

5.3.1.1.5 Host Bus Adapters

The CJIS Broker Database Servers each contain Host Bus Adapters (HBA) which allows the Database Servers to store, manipulate, and retrieve data on the ITE SAN. Dual channel HBAs have been selected to provide maximum performance along with single card fault tolerance. Utilization of the SAN is only proposed and priced for the high-end solution, but it could also be deployed to the servers priced in the lower end configuration. The price is the same regardless of the price of the physical server type being connected to the SAN.

The following table depicts the cost for the Host Bus Adapters.

			Low-End Option			High-End Option
Description	**Units Required**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
HBA for Database Server	0	$1,500.00	$0.00	6	$1,500.00	$9,000.00

The high-end configuration includes card-level fault tolerance by allocating two dual channel HBAs in each server. This allows each Database Server to maintain SAN connectivity in the event of a HBA card failure.

5.3.1.1.6 Firewalls

The firewall devices will be utilized to provide secured and encrypted VPN connections between participants' web service layers and the centralized broker. Such devices provide the point-to-point secured connectivity without the need for user-supplied credentials for each transaction. DOC and DPS already have firewalls in addition to the ICN firewalls used to segregate raw Internet traffic. Presented are estimates for Judicial, JDW, and the central broker system itself.

The following table depicts the low-end units and cost as well as the high-end units and cost for the firewall devices.

	Low-End Option			High-End Option		
Description	**Units Required**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
Firewalls	3	$8,000.00	$24,000.00	4	$32,000.00	$128,000.00

5.3.1.2 Network Infrastructure Costs

The CJIS Broker will require a connection to a network for the purposes of exchanging information between the participating systems. The connection options include a broadband connection using a VPN or a dedicated T1 line. The estimate includes both one-time setup fees and the expected recurring costs for the connection and the JFHQ services necessary to support the expected information exchange to be handled.

The following table depicts the low-end units and the high-end cost for the one-time setup fee for network costs.

Network One-time Fee	**Low-End Option - VPN**			**High-End Option - T1 Connection**		
Description	**Units Required**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
User Connection	1	$174.00	$174.00	1	$1,643.00	$1,643.00
JFHQ Services	1	$2,540.00	$2,540.00	1	$2,000.00	$2,000.00
Total			**2,714.00**			**3,643.00**

The following table depicts the low-end units and the high-end recurring costs for the network connectivity.

Network Recurring Cost	Low-End Option - VPN			High-End Option - T1 Connection		
Description	**Units Required**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
User Connection	12	$110.00	$1,320.00	12	$879.00	$10,548.00
JFHQ Services	12	$2,161.00	$25,932.00	12	$2,744.25	$32,931.00
Total			**27,252.00**			**43,479.00**

An effort to determine if there are network connectivity needs beyond the broker necessary to carry the expected traffic should be made early in the design phase of the solution. If additional connections are necessary, these same numbers can be used for each additional connection to be included in the costing effort.

5.3.1.3 CJIS Broker Software Costs

5.3.1.3.1 SAN TSM Client

The SAN TSM Client software could be utilized to provide server backup functionality for CJIS Broker servers. CJIS business data, such as hot files would not be backed up via the SAN TSM Client. The TSM Client provides client backup such as server operating system, server configuration, and application program logic. This software configuration is not being proposed in the low-end cost range, but the configuration of the functionality in the lower end servers being proposed is available. The license for the software is available to subscribers using the SAN from ITE.

The following table depicts the low-end units and cost as well as the high-end units and cost for the SAN TSM Client software.

	Low-End Option			High-End Option		
Description	**Units Required**	**Unit Cost**	**Total Cost**	**Units Required**	**Unit Cost**	**Total Cost**
SAN TSM Client	0	$218.40	$0.00	15	$218.40	$3,276.00

It should be noted that each server being deployed in the high-end configuration is expected to have the TSM Client for OS/configuration backup purposes.

5.3.1.3.2 SAN High Availability Data Protection Package

The SAN High Availability Data Protection Package will be utilized to provide additional data protection for specialized data formats in the high-end configuration if it is deemed appropriate in the detailed requirements of the CJIS Broker. As with the other parts of the SAN functionality, it could be deployed to the low-end server, but it has not been included in the configuration cost of such an approach.

The following table depicts the low-end units and cost as well as the high-end units and cost for the SAN High Availability Data Protection Package software.

	Low-End Option			High-End Option		
Description	**Units Required**	**Unit Cost**	**Total Cost**	**Units Required**	**Unit Cost**	**Total Cost**
SAN High Availability Data Protection Package	0	$1,116.16	$0.00	6	$1,116.16	$6,696.96

5.3.1.3.3 OS Cluster Software

The Operating System (OS) Cluster software will be utilized to provide OS Clustering of the Database Servers to ensure a highly available, fault tolerant, and load-balanced database solution. A lower cost solution is priced, but it is not included in the low-end configuration, as this configuration is only depicted in the high-end solution.

The following table depicts the low-end units and cost as well as the high-end units and cost for the OS Cluster software.

			Low-End Option			High-End Option
Description	**Units Required**	**Unit Cost**	**Total Cost**	**Units Required**	**Unit Cost**	**Total Cost**
OS Cluster Software	0	$499.00	$0.00	2	$60,000.00	$120,000.00

5.3.1.3.4 Database

The Database software will be utilized to provide RDBMS data storage functionality in the CJIS Broker. Due to the criticality of the storage and retention of data within the CJIS Broker, an advanced, highly reliable, highly scalable RDBMS is recommended if the CJIS Broker will be responsible for carrying out mission critical functionality required in a 24X7 environment. The SAN High Availability Data Protection Package and Database Clustering are also recommended in these mission critical deployments.

The following table depicts the low-end units and cost as well as the high-end units and cost for the Database software.

			Low-End Option			High-End Option

Description	Units Required	Unit Cost	Total Cost	Units Required	Unit Cost	Total Cost
Database Server Software	3	$32,000.00	$96,000.00	6	$32,000.00	$192,000.00

The Database Servers contain the Database software, however it should be noted that the data files in the high-end configuration utilized (e.g., physical files CJIS Broker data resides in) the SAN and not on the Database Server.

5.3.1.3.5 Database Clustering

Database Clustering software will be utilized to provide Database level clustering of the Database Servers in the production regions of the high-end configuration. This provides a highly available, scalable, and reliable Database server for the CJIS Broker.

The following table depicts the low-end units and cost as well as the high-end units and cost for the Database Clustering software.

	Low-End Option			High-End Option		
Description	Units Required	Unit Cost	Total Cost	Units Required	Unit Cost	Total Cost
Database Clustering Software	0	$16,000.00	$0.00	4	$16,000.00	$64,000.00

5.3.1.3.6 Web/Application Server Software

The Web/Application Server for the CJIS Broker is recommended to be a J2EE environment utilized to produce the User Interface for the CJIS Broker. The functional components of the system would include use by County Attorneys in support of e-filing and other administrative functions requiring a user interface to the CJIS Broker. In the low-end solution this is recommended to be open source software compliant with the J2EE requirements. The software is free of charge, but support and maintenance can be purchased. The Web/Application Server software will also contain logic to communicate with other business logic applications in the same manner as the automated applications interfaces to provide a seamless user interface for the CJIS Broker.

The following table depicts the low-end units and cost as well as the high-end units and cost for the Web/Application Server for UI software.

			Low-End Option			High-End Option
Description	**Units Required**	**Unit Cost**	**Total Cost**	**Units Required**	**Unit Cost**	**Total Cost**
Application Server Software	1	$0.00	$0.00	2	$9,000.00	$18,000.00

5.3.1.3.7 Service-Oriented Architecture Platform Software

The Service-Oriented Architecture Platform Software will be utilized to provide the business rule processing for the CJIS Broker. The primary components of such software are a centralized, scalable, fault-tolerant, service-messaging framework. The software provides for communicating with heterogeneous services (e.g., CORBA, Web Services) over a diverse set of message protocols. It should establish a shared messaging layer that enterprise applications, services, and components can utilize to connect and communicate the IEP to be implemented in Iowa over the next five years. The initial rollout of the CJIS broker will focus on asynchronous messaging, but the Service-Oriented Architecture Platform Software must be capable of implementing asynchronous message types. These messages will require a secure transmission and the software should provide sophisticated error recovery, allowing for failed message delivery, scalability issues, and other messaging issues that will occur in a SOA environment. The components of these platforms consist of multiple components that typically include the following:

- User Interface for development of the message exchanges
- Repository of business rules developed for message brokering
- Run-time Engines that run in a J2EE or .NET platform

A variety of pricing configurations are possible from the multitude of vendors offering solutions in this area. The prices below are intended to provide approximate cost for the Service-Oriented Architecture Platform Software. The following table depicts the low-end units and cost as well as the high-end units and cost for the Service-Oriented Architecture Platform Software.

			Low-End Option			High-End Option
Description	**Units Required**	**Unit Cost**	**Total Cost**	**Units Required**	**Unit Cost**	**Total Cost**
SOA Platform Server Software	3	$40,000.00	$120,000.00	5	$125,000.00	$625,000.00

5.3.1.4 Adapters and Data Exchange Development

To achieve the objectives of the Iowa CJIS initiative, the ability to send and receive transactions between loosely coupled systems must be created as part of the justice environment. To facilitate automated exchange between the various systems in the Iowa CJIS enterprise, each participating application will require a transaction exchange layer within its current architecture. This exchange layer for each participating application will consist of two major components:

- A re-usable adapter framework, or interface environment, in which data exchanges can be sent from the participating application and received from other participating applications
- A business processing layer that has the ability to know when to generate data exchange, and how to process data exchanges received from outside entities according to the business rules of the agency it supports

Ideally, this layer would be constructed of an area of web services, but this will not necessarily be achievable in every participating application. In those applications where constructing a custom web service layer is not achievable, COTS software can be purchased to achieve the necessary processing capability. Once the adapter framework is in place, each data exchange will require programming logic to either send the transaction, or process a transaction being received. The cost for the framework is a one-time procurement, as is the implementation of each data exchange. The cost being illustrated is on a per application, per exchange basis. The actual dollar amount will depend on the number of participating applications, and the number of exchanges deployed to each.

The following table depicts the low-end and high-end Adapter Framework and Data Exchange development costs.

	Low End Option			High-End Option		
Description	**Units Required**	**Unit Cost**	**Total Cost**	**Units Required**	**Unit Cost**	**Total Cost**
Adapter Framework	15	50,000.00	$750,000.00	30	$100,000.00	$3,000,000.00
Data Exchange	50	1,000.00	$50,000.00	100	$3,000.00	$300,000.00
Total			**$800,000.00**			**$3,300,000.00**

5.3.1.5 CJIS Broker Implementation Project Costs

The implementation of the CJIS Broker can be accomplished by either the procurement of a COTS solution, or a custom developed application. There is not an end-to-end COTS solution available at this time that would fulfill the functional requirements sought and described in the To-Be Technical Analysis. Individual pieces of the solution may be

purchased or developed, but they will require custom programming to integrate the disparate components. For pricing purposes, the solution is being illustrated as custom development effort, however, if the functionality is procured, portions of the implementation budget should provide a comparable measure of cost.

The project estimated is an 18-month engagement through a full system development life-cycle, which would be procured in the beginning of Year Two, assuming a General Fund appropriation from the Iowa Legislature. It accounts for resource costs for the design, development, testing, and implementation of CJIS Broker as defined in the To-Be Environment. It is assumed that a full functional requirements definition has been performed prior to the project, and a full scope of the system has been documented and accepted by the CJIS Board, CJIS Advisory Committee, and Iowa CJIS Program Office. The project uses a mix of resources:

- Managers – Handle planning, project management, oversight and execution of the system development life-cycle
- Senior System Analysts/Developers – Seasoned and knowledgeable resources modeling and programming the application according to the requirements gathered in interviews and reference material
- System Analysts/Developers – Resources assisting in the modeling and programming of the application
- Trainer/Writer – Resources helping document the solution and providing any training necessary for the use of the system by the envision user groups, administrators, and managers

Two options are provided for the effort. The first is utilizing ITE program resources at the FY05 published rates. The second is procuring the services from a third-party vendor through a competitive bid and award of a contract.

The following table illustrates the expected system development life-cycle costs.

CJIS Broker Development			ITE Resources		Vendor Resources	
Labor Category	**Resource Hours**	**Number of Resources**	**Hourly Rate**	**Project Cost**	**Hourly Rate**	**Project Cost**
Manager	2100	3.00	$141.01	$888,363.00	$150.00	$945,000.00
SR System Analyst/Developer	2005	5.50	$84.59	$932,604.75	$125.00	$1,378,125.00
System Analyst/Developer	2005	5.50	$68.99	$760,614.75	$100.00	$1,102,500.00
Trainer/Writer	2100	1.50	$68.99	$217,318.50	$100.00	$315,000.00
Total				**$2,798,901.00**		**$3,740,625.00**

The determination of the approach will need to be established in the initial stages of the five-year integration plan. Some of the considerations that should be researched are:

- Amount of applicable technical knowledge required in the platforms selected for deployment of the CJIS Broker
- Business acumen necessary from the design, development, and implementation staff necessary to assure success of the project

5.3.1.6 Law Enforcement Gateway/TraCS Repository

The MAXIMUS/URL Team proposes the creation of a law enforcement gateway and persistent TraCS repository to support the participation of local law enforcement agencies (using either RMS or TraCS) in the CJIS solution. Specifically, we recommended that as part of this project, a centralized middle tier layer to support web services for all local law enforcement agencies be developed and implemented at DPS. It is also anticipated that in Year Two, DOT will have purchased and developed the method for creating SOAP messages for TraCS exchanges and a persistent storage mechanism for TraCS XML documents.

This recommendation is consistent with the Cisco audit provided to DOT in May 2005. It includes a cost estimate for the initial web services development at DPS as well as the TraCS Repository itself. The hardware and software costs for the Law Enforcement Gateway/TraCS Repository is outlined and accounted for in Section 5.1.1.1, CJIS Broker Hardware Costs.

DPS Gateway and TraCS Central Repository			**ITE Resources**		**Vendor Resources**	
Labor Category	**Resource Hours**	**Number of Resources**	**Hourly Rate**	**Project Cost**	**Hourly Rate**	**Project Cost**
Manager	900	1.00	$141.01	$126,909.00	$150.00	$135,000.00
SR System Analyst/Developer	900	1.00	$84.59	$76,131.00	$125.00	$112,500.00
System Analyst/Developer	900	2.00	$68.99	$124,182.00	$100.00	$180,000.00
Trainer/Writer	450	0.50	$68.99	$15,522.75	$100.00	$22,500.00
Total	**3150**			**$342,744.75**		**$450,000.00**

5.3.1.7 Implementation Cost Summary

The one-time costs for the State of Iowa CJIS Integration Plan are summarized in the table below. One-time costs for the ITE setup is discussed in the Recurring Operational Costs section that follows.

Category	Low-End Cost	High-End Cost
Hardware	$159,477.05	$763,588.70
Software	$216,000.00	$1,028,972.96
System Development	$3,141,645.75	$4,190,625.00
Adapter Framework	$800,000.00	$3,300,000.00
ITE One-Time Set Up Fee	$19,734.00	$48,863.80
Network Infrastructure Set up Fee	$2,714.00	$3,643.00
Total	**$4,339,570.80**	**$9,335,693.46**

5.3.2 Recurring Operational Costs

The recurring operational costs provide costing scenarios for the ongoing activities that will be required to achieve the five-year CJIS Integration Plan. The operational categories presented include maintenance costs for software and hardware components of the solution, ITE hosting of the CJIS Broker, and labor costs for the CJIS Program Office staff. Like the one-time costs, these recurring operational costs have a low-end and high-end range, as the maintenance costs are driven off a percentage of the software and hardware procurement fees, or there is a salary range applicable to the positions being recommended.

5.3.2.1 Ongoing Software License and Hardware Maintenance Costs

Ongoing software license and hardware support will be an annual procurement for the CJIS Broker. The following table illustrates the costs associated with the low- and high-end configurations. A standard rate of 18% of the original procurement is used to calculate the approximate cost that should be expected to be renewed annually. Actual rates may vary depending on the software and hardware selected for the implementation. The cost of the license and hardware support should be included in the first year purchase and not incurred until the second year of ownership.

			Low-End Option			High-End Option
Description	**% Cost**	**Item Cost**	**Yearly charge**	**% Cost**	**Item Cost**	**Yearly charge**
Central Broker Hardware						
Application Server	18.00%	$9,098.72	$1,637.77	18.00%	$59,985.00	$10,797.30
XML Accelerator	18.00%	$0.00	$0.00	18.00%	$105,000.00	$18,900.00
SOA Platform Server	18.00%	$27,296.16	$4,913.31	18.00%	$119,970.00	$21,594.60
Database Server	18.00%	$99,082.17	$17,834.79	18.00%	$341,633.70	$61,494.07
HBA for Database Server	18.00%	$0.00	$0.00	18.00%	$9,000.00	$1,620.00
Central Broker Software						
SAN TSM Client	18.00%	$0.00	$0.00	18.00%	$3,276.00	$589.68
SAN High Availability Data Protection Package	18.00%	$0.00	$0.00	18.00%	$6,696.96	$1,205.45
OS Cluster Software	18.00%	$0.00	$0.00	18.00%	$120,000.00	$21,600.00
Database	18.00%	$96,000.00	$17,280.00	18.00%	$192,000.00	$34,560.00
Database Clustering	18.00%	$0.00	$0.00	18.00%	$64,000.00	$11,520.00
Application Server Software	18.00%	$0.00	$0.00	18.00%	$18,000.00	$3,240.00
SOA Platform Server Software	18.00%	$120,000.00	$21,600.00	18.00%	$625,000.00	$112,500.00
Total			**$63,265.87**			**$299,621.10**

5.3.2.2 ITE Hosting Costs

The ITE hosting costs present two areas of services to be provided by ITE for the CJIS Broker solution. First, the costs for hosting of the CJIS broker hardware and software components are delineated for the low-end and high-end options. The second service area presented are the Storage Area Network (SAN) represented in the system hardware profile (see Section 5.1.1.1 CJIS Broker Hardware Costs).

ITE offers a variety of options for the hosting of other agencies servers. The costing presented is consistent with the To-Be Environment recommendations for deployment of the CJIS Broker in Iowa and meet the requirements for a high availability mission critical system. The figures presented are based upon ITE's advertised rated for Server Farm Services (http://www.state.ia.us/government/ite/rates_FY05/server_farm.html) and includes both the initial setup fees for the servers and the ongoing monthly charges for the deployed servers. As with the cost categories, both the low-end option and high-end option are illustrated in the table below to ensure the range of cost for the hosting environment takes in to account the multiple configurations that may comprise the best Iowa CJIS Solution.

Description of Service	Charge Type	Cost Per Unit of Charge Type	Charge Units Required	Low-End Option		High-End Option	
				Applicable Hardware Units	Annual Cost	Applicable Hardware Units	Annual Cost
Hosted Environment Costs							
Rack/Server Configuration	Hourly	$98.67	40	5	$19,734.00	11	$43,414.80
Logical Server Hosting	Monthly	$390.09	12	5	$23,405.40	11	$51,491.88
Physical Server Hosting	Monthly	$169.60	12	5	$10,176.00	11	$22,387.20
Special System Monitoring	Monthly	$390.09	12	5	$23,405.40	11	$51,491.88
One-Time Environment Set up Fee					**$19,734.00**		**$43,414.80**
Hosted Environment Annual Costs after First Year					**$56,986.80**		**$125,370.96**

The largest driver for cost is the number of servers being deployed. Configurations with more or less physical servers will impact the cost. The Rack/Server Configuration line item is a one-time cost of locating and configuring the servers in the ITE Server Farm. After the first year of costs, a reduction in the ITE charges for hosting the environment will be realized if the monthly rates remain the same.

As explained in the CJIS Broker Hardware Costs Section, the use of the ITE SAN for network backup and database server storage is a component of the high-end option. Other options such as a RAID disk configuration could be utilized on the low-end, but are not as capable for a system with the mission critical functionality being provided in the CJIS Broker. The following table illustrates the SAN costs for both configurations.

Description of Service	Charge Type	Cost Per Unit of Charge Type	Charge Units Required	Low-End Option Applicable Hardware Units	Low-End Option Annual Cost	High-End Option Applicable Hardware Units	High-End Option Annual Cost
SAN Cost							
Network-Based Backup and Restore							
Set up Fee	Fixed	$253.82	1	0	0.00	11	$2,792.02
Server Charge	Monthly	$157.77	12	0	0.00	11	$20,825.64
SAN Costs Basic Package							
Set up Fee	Fixed	$253.82	1	0	0.00	6	$1,522.92
Server Charge	Monthly	$315.54	12	0	0.00	6	$22,718.88
Unlimited Storage - High Availability Option							
Set up Fee	Fixed	$62.10	1	0	0.00	6	$372.60
Server Charge	Monthly	$315.54	12	0	0.00	6	$22,718.88
Unlimited Storage - Data Protection Option							
Set up Fee	Fixed	$126.91	1	0	0.00	6	$761.46
Server Charge	Monthly	$315.54	12	0	0.00	6	$22,718.88
SAN One-Time Set Up Fee					**0.00**		**$5,449.00**
SAN Annual Costs after First Year					**0.00**		**$88,982.28**

As with the Server Farm hosting, the number of physical boxes being deployed in the environment is the greatest driver of the cost. Also, there will be a one-time set up fee incurred in the first year that will not be applicable in the remaining years. The difference in the costs is illustrated in the last two rows of the table.

5.3.2.3 CJIS Program Office Operational Costs

If the recommendations for the establishment of the CJIS Program Office are adopted, staffing for the office will require legislative funding. The table below provides the expected positions, salary grades, and operational support requirements for the new positions. It also contains annual costs for the Project Manager, which is an Executive Officer 3 position currently funded by a general fund appropriation to CJJP.

		Low-End Option			High-End Option		
Labor Category	**Operational Support**	**Annual Wage**	**Benefits**	**Annual Cost**	**Annual Wage**	**Benefits**	**Annual Cost**
CJIS Project Manager	Already Funded Position			$121,334.00			$121,334.00
GJXDM Exchange Modeler	9,500.00	$53,892.80	$11,317.48	$74,710.28	$80,870.40	$16,982.78	$107,353.18
CJIS Broker System Developer	9,000.00	$46,550.40	$9,775.58	$65,325.98	$70,241.60	$14,750.73	$93,992.33
Help Desk	8,500.00	$35,755.20	$7,508.59	$51,763.79	$52,977.60	$7,508.59	$68,986.19
Total				**$313,134.05**			**$391,665.70**

5.3.2.4 Recurring Operational Cost Summary

The following table illustrates the expected ongoing operating costs that will be incurred if the State of Iowa CJIS Integration Plan is executed as recommended.

Category	**Low-End Annual Cost**	**High End Annual Cost**
CJIS Program Office	$313,134.05	$391,665.70
Hardware Software Maintenance	$63,265.87	$299,621.10
ITE Hosting	$56,986.80	$214,353.24
Network Infrastructure	$27,252.00	$43,479.00
Total	**$460,638.72**	**$949,119.04**

5.3.3 Five-Year Plan Spending Rates

The following table represents the total costs associated with each year of the strategic plan. The expenditures indicated are based on the yearly activities described in detail in the Implementation Strategy document.

	Low-End Solution				High-End Solution			
Year	**Total**	**% of Project**	**One-Time Expenditure**	**Recurring Cost**	**Total**	**% of Project**	**One-Time Expenditure**	**Recurring Cost**
Fiscal Year 06	$357,666.42	6%	$261,377.70	$96,288.72	$690,804.88	6%	$569,466.85	$121,338.03
Fiscal Year 07	$1,963,416.90	33%	$1,607,356.93	$353,345.97	$3,888,015.83	32%	$3,387,417.21	$496,955.62
Fiscal Year 08	$1,892,040.70	32%	$1,471,268.98	$420,771.72	$3,657,149.05	31%	$2,881,466.76	$775,682.29
Fiscal Year 09	$889,786.35	15%	$447,499.48	$442,286.87	$1,961,875.78	16%	$1,089,852.90	$872,022.89
Fiscal Year 10	$882,511.15	15%	$421,872.43	$460,638.72	$1,791,673.42	15%	$842,554.38	$949,119.04
Total	**$5,985,421.51**	100.00%	**$4,209,375.51**	**$1,773,331.99**	**$11,989,518.97**	**100%**	**$8,770,758.10**	**$3,215,117.87**

6 Performance Metrics

The Performance Metrics section will provide a definition and discussion of performance measurement in a justice environment. It will then discuss specific performance measures that the Iowa CJIS effort could undertake to map to the goals and objectives defined by the CJIS Board and Advisory Committee.

6.1 Background of Performance Metrics in a CJIS Environment

According to the Center for Society, Law, and Justice (CSLJ), a not-for-profit organization that has published a number of documents on how to quantify performance and the benefits of information sharing in a justice environment, a performance measure is "a quantitative or qualitative characterization of performance: a measure of the achievement of an objective of an organization or activity." Furthermore, performance measurement systems typically measure the following:

- Inputs: resources consumed by an agency's activities;
- Outputs: products or services produced by a program or process and delivered to customers (which might include other programs or processes within the agency); and/or
- Outcomes: expected, desired, or actual results to which outputs of the activities of an agency have an intended effect.[46]

While measuring performance in private sector organizations has been the norm in the business world, quantifying the performance of public programs has largely been thought to be much more challenging, as results and outcomes of public sector programs are often difficult to quantify. However, in the past 20 years there has been a significant trend at all levels of government to measure the performance of government agency inputs, outputs, and outcomes. The Government Performance and Results Act (GPRA) was enacted in 1993 and requires federal agencies to develop strategic plans for how they would deliver high-quality products and services to the American people. Under GPRA, strategic plans are the starting point for each federal agency to (1) establish top-level agency goals and objectives, as well as annual program goals; (2) define how it intends to achieve those goals; and (3) demonstrate how it will measure agency and program performance in achieving those goals.[47]

[46] *Performance Measurement Tools for Justice Information Technology Projects: Key Issues in Developing Performance Measurement Systems Justice Integration*, U.S. Department of Justice, Bureau of Justice Statistics and the Center for Society, Law, and Justice at the University of New Orleans, DRAFT, page 6 (hereinafter *CSLJ Performance Measures*).

[47] *Serving The American Public: Best Practices In Performance Measurement*, White House Office of National Performance Review, June 1997, at http://www.orau.gov/pbm/links/npr2.html.

This trend toward government accountability and its ability to provide outcome-based measures of spending and performance permeated state and local governments as well, especially as decision makers and justice practitioners began thinking about how justice information systems could be better integrated. This effort has become increasingly important in recent years, due to budget shortfalls, especially at the state and local level. More and more, decision makers are looking to ensure the programs and initiatives they support demonstrate their intended effect and in many cases, also establish a return on investment in order to justify a continued investment. According to an article in the National Association of State Chief Information Officers (NASCIO) publication *Government Information Sharing: Calls to Action – Justice Perspectives*, "incorporating performance measures into justice information sharing initiatives is critical to effectively monitoring project implementation and demonstrating success toward achieving long-term goals and outcomes." Furthermore, the article suggests performance measures should be used to:

- Establish a baseline for demonstrating results;
- Align project goals with policy strategies;
- Make project goals operational;
- Provide for benchmarking; and
- Ensure cost effective returns on investment.[48]

The State of Iowa is regarded as a national leader in the area of performance measures, especially in the area of information technology investment. The State of Iowa uses the Return On Investment (ROI) Program to evaluate Information Technology (IT) projects and expenditures since 2000, when Governor Vilsack asked the Iowa Department of Administrative Services, Information Technology Enterprise (ITE) to construct a methodology for evaluating the benefits of information technology (IT) projects in Iowa State government. These benefits are those that accrue to Iowa citizens, to State government, or to both. The Governor wanted to know the extent to which IT projects are projected to deliver or actually have delivered a bona-fide "return on investment."[49] Since the ROI Fund's inception, it has provided over $920,000 for CJIS in Iowa, which was used to support upgrades to the DOC's ICON and DPS IOWA System to make them more "integration ready" as well as to support the CJIS project management function and for the state match for federal grants to support the CJIS effort.

6.2 Types of CJIS-Based Performance Measures

The U.S. Department of Justice, Office of Justice Programs (OJP) has supported work to assist justice organizations and in planning for and implementing CJIS efforts with performance measurement in mind. According to *Performance Measurement Tools for Justice Information Technology Projects: Key Issues in Developing Performance*

[48] *Government Information Sharing: Calls to Action – Justice Perspectives*, National Association of State Chief Information Officers (NASCIO), March 2005, page 30.
[49] Iowa Return on Investment (ROI) Program website, at http://das.ite.iowa.gov/roi/index.html.

Measurement Systems Justice Integration, a performance measurement system should flow from an organization's mission and strategic plan. However, justice system integration projects, by definition, involve more than one organization. A project may be part of an overall program to build an integrated information system, and that program may implement, or be part of, a strategic plan for integration in a city, county, or state. Each type of agency involved has its own unique mission and goals, and even agencies of the same type will often differ on which goals are emphasized.[50]

Beyond settling on strategic goals and objectives, the development of outcome-based performance measures for justice integration necessarily involves something far more tangible: the use of the shared data and information that each agency uses as part of its day-to-day business process and workflow in achieving its mission. Identifying these measures is a two-part process. The first step is to establish a baseline, which will measure the current criminal justice process and outcomes based on the current state of criminal justice information sharing in Iowa. The second step is to identify valid ways in which these same baseline measures may be captured in an integrated environment. The collection of these measures in an automated environment will provide a perspective on how the automation has improved the administration of justice in the State. Collecting this data consistently over the course of the CJIS implementation will also identify how the process and outcomes improve as more agencies participate in the CJIS solution and more exchanges are moved to a transaction-based, real-time workflow. Developing both baseline and post-implementation measures is a collective effort that requires collaboration and consensus among all integration partners.

According to the CSLJ, there are several types of performance measures applicable to an integrated justice environment. They include:

- Project measures, which are direct measures of whether a project-planning task has been started or completed. Examples include project management-related issues, such as progress in securing resources, establishing governance structures, design, planning, and implementation;
- Measures of integration that address information availability, operational quality, and information flow;
- Information processing measures, which address information quality such as errors, redundant data entry, and allowing for more timely and complete summary records; and
- Measures that improve public safety. These measures can be reflective of improvements in an agency's core mission (accurate and more efficient arrest process, for example) as well as measures of overall public safety such as reductions in crime rate and citizen satisfaction.[51]

[50] *CSLJ Performance Measures,* pages 13-14.
[51] *CSLJ Performance Measures,* pages 10, 18, 22, 32.

The Iowa CJIS governance documents as well as the RFP issued for the development of this strategic plan outlined several goals and objectives for improved efficiency and effectiveness that the State expects to derive benefit from as a result of implementing justice information sharing in Iowa. These goals and objectives align with many of these measures as identified above, and the section below will offer specific suggestions for performance measures in the areas that are priorities for the Iowa CJIS effort.

6.3 CJIS Objectives

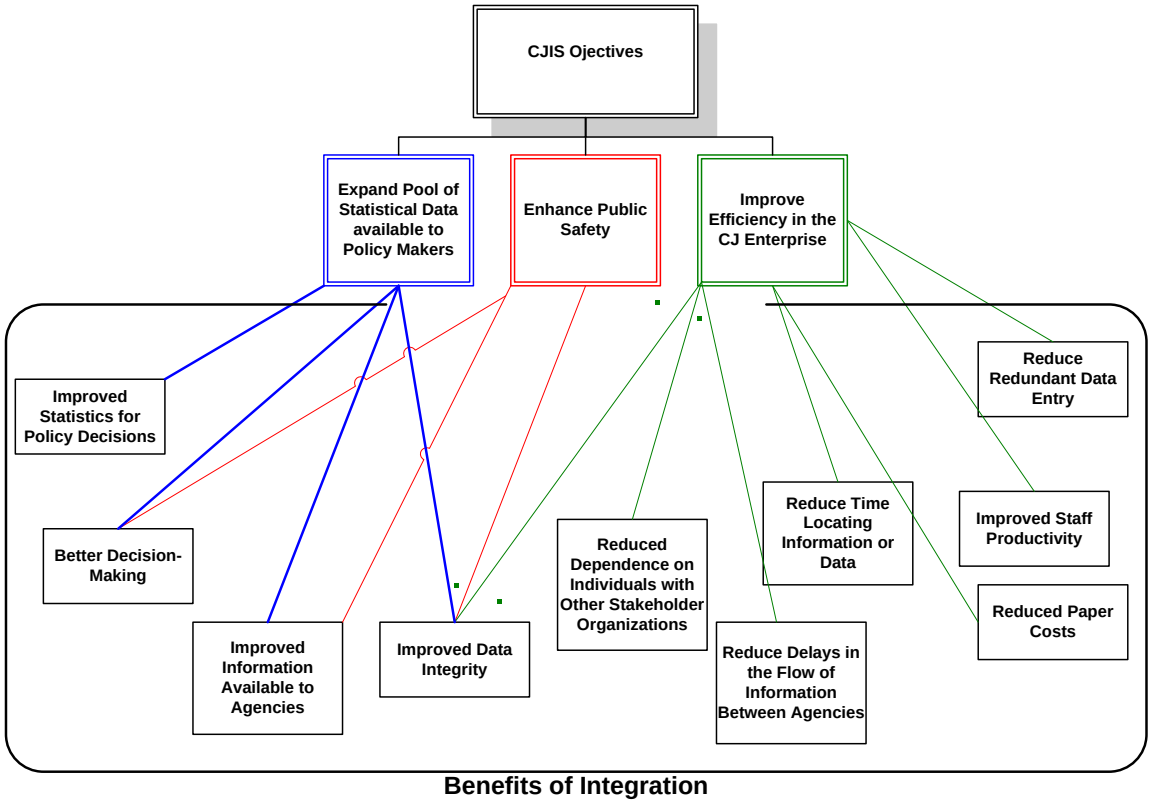
The State of Iowa's CJIS Governance Memorandum of Understanding (MOU) states that the State will achieve a positive return on investment from integration; not only in increased public safety but also through improved process management, agency communication, information quality and access, and criminal information for decision-making. Specifically, the MOU notes that the State recognizes that "The development of a statewide integrated justice information system would achieve many important objectives:

- It would enhance public safety by providing criminal justice agencies and officials, including police officers, judges, and corrections officers, with faster access to important criminal justice information at critical points in the justice process;
- It would improve the efficiency of criminal justice agencies by reducing redundant data collection and entry, and by reducing or eliminating labor intensive, time-consuming paper-based processes; and
- It would expand the pool of statistical data available to state and local officials for making and evaluating public policies."

Furthermore, the CJIS Strategic Plan RFP identified specific performance goals expected from a CJIS implementation, which had been previously identified in the URL Integration Adult Exchange Analysis:

- Better Decision-Making
- Reduced Redundant Data Entry
- Reduced Delays in the Flow of Information Between Agencies
- Improved Information Available to Agencies
- Improved Staff Productivity
- Reduced Paper Costs
- Reduced Dependence on Individuals With other Stakeholder Organizations
- Reduced Time Locating Information or Data
- Improved Data Integrity
- Improved Statistics for Policy Decisions

The following graphic maps these goals to the overall objectives outlined in the MOU. Each goal will be discussed in turn, with an example of measures that could be implemented in order to measure the effectiveness of the CJIS solution in achieving it. For these goals and objectives, there is a combination of outcome and process-based measures that are presented.



Benefits of Integration

6.3.1 Expanding Pool of Statistical Data Available to Policy Makers

This CJIS objective includes the goals of better decision-making, improved information available to justice agencies, improved data integrity, and improved statistics for policy decisions. Justice integration improves the information available to policymakers by facilitating access to better quality and more timely information. This leads to better decision-making, better reporting, and better policies based on real information. Measures associated with this Iowa CJIS objective include measures of integration that address information availability, operational quality, and information flow and integration processing measures, such as data error reduction.

6.3.1.1 Better Decision Making

Measurable objectives associated with improved decision making include:

- Tracking the amount of time it takes to enter a Court Disposition into the State Criminal History Repository

- Monitoring the amount of missing data among the governmental entities
- Monitoring the number of data errors reported for correction for current information exchanges
- Measuring the amount of time it takes to enter a warrant into the IOWA System
- Measuring the amount of time it takes to enter a Protective Order into the IOWA System.[52]

6.3.1.2 Improved Information Available to Criminal Justice Agencies

Currently, only necessary information is passed between agencies. In addition, it has been well documented in the earlier exchange studies that many business processes and forms in Iowa are jurisdiction dependent. For example, the URL Adult Exchange Analysis found that "...the business practices at the local level differ between jurisdictions. The roles of law enforcement, the Prosecutor, the Court, and Community Corrections are not consistent, which has forced the Courts to adapt the ICIS system to each of the different processes." The recommendation that followed was to make the interactions with ICIS consistent across jurisdictions in order to facilitate more sharing of more information among more agencies.

In addition to receiving increased accurate information in a more timely fashion, automation facilitates the receipt of more criminal and case information than in the past. As a result of the exchange mapping process, URL discovered a number of notifications, notices, and documents that agencies would like to receive. This information can be made available within the justice system once it is integrated and easier to send and receive data between agencies.

Increased availability of information can be measured by user access measures, including an increase in the number of agencies with automated systems. Iowa-specific examples, based on the recommendations set forth in this plan, could include:

- Change in the number of TraCS users
- Change in the number of County Attorneys' offices with an automated case management system
- Change in the number of arrests submitted by Livescan
- Monitoring system access and usage
- Change in the volume of existing electronic exchanges (such as Protection Orders, PSI)
- Change in the number of users of the CJIS Broker
- Change in the numbers of queries to the CJIS Broker

[52] Performance MetrCJIS Broker In Integrated Justice: Measuring Success And The Need For Improvement, 2002 SEARCH Symposium, presentation by Bob Roper, CIO, Colorado Judicial Branch and Teri Sullivan, SEARCH, at www.it.ojp.usdoj.gov (hereinafter *SEARCH Presentation*).

6.3.1.3 Improved Data Integrity

It is clear that within the State of Iowa there are several instances where duplicate entry takes place. Integration will greatly improve data integrity since redundant data entry and manual data entry efforts are prone to error. Also, the enhancement of some of the processes such as efforts to increase disposition matching rates will improve the integrity of the data, improve criminal history records, and ultimately help law enforcement track and apprehend criminals. Data will be readily available, diminishing the need to look in several places to confirm or acquire information. It can also improve decision-making since more or additional information will be available in a timely manner.

Examples of measures associated with improving data integrity include:

- Change in disposition matching rates
- Change in number of incidents where criminal records are associated with the wrong person
- Change in the number of situations in which criminal records are associated with the wrong person
- Change in time from arrest to adjudication
- Change in amount of missing data among criminal justice entities
- Measurement of the discrepancy between active warrants ICIS and those on the IOWA System
- Change in number of incidents where wrong person is released from custody

6.3.1.4 Improving Statistics for Policy Decisions

On a policy level, decision making is dependent largely on the analyses performed by CJJP based on information that resides in the Justice Data Warehouse. Currently, CJJP receives most of its information from batch file transfers from the Judicial Branch and Department of Corrections once a month. For the latter, a complex algorithm is performed to upload the data from the ICON system to the data warehouse. In addition, significantly more analysis is necessary to link Judicial and Corrections data within the data warehouse.

If more information were exchanged systemwide, the information stored individually by the Judicial Branch and DOC that could be shared with the warehouse would likely be richer and more timely. In addition, it is likely that more agencies could contribute information to the JDW more easily and quickly. This would result in more timely and accurate information in the JDW and for policymakers to base their decisions about the justice enterprise.

6.3.2 Enhancing Public Safety

In addition to those measures listed above, there are several outcome-based measures that seek to measure improvements in public safety as a result of justice information sharing.

- Change in percentage of court dispositions that match to an arrest incident
- Change in the number of times Court dispositions are not reported in criminal histories
- Change in average response time it takes to receive a positive identification
- Change in the recidivism rate
- Change in the amount of time it takes to issue victim notices
- Measuring the likelihood of convicted and/or registered sex offenders who find employment in sensitive positions
- Change in the clearance rate for crimes against persons
- Change in conviction rate
- Measuring the percentages of arrests compared to active warrants related to serious criminal activity

6.3.3 Improving Efficiency in the Criminal Justice Enterprise

Efficiency in the criminal justice enterprise includes several process related goals, such as reducing redundant data entry, reducing paper costs, reducing the dependency on specific individuals within the organization, and improving staff productivity. The measures associated with these goals focus on improving the availability of information and the amount of time that current staff spends on entering information in their own systems and verifying the information received from other agencies.

6.3.3.1 Reducing Redundant Data Entry

Reducing redundant data entry is a measure of the quality of justice information. Integration is intended to improve information quality by eliminating redundant data entry, allowing better error checking, and allowing for more timely and complete summary records such as criminal histories. However, integration is much easier if data is standardized, accurate, and complete.

Currently, this process can be measured by the time it takes for a Court Clerk, for example, to re-enter case filing information that it receives from either law enforcement or the County Attorney, multiplied by the volume of filings the office receives per day, week, month, or year. An automated exchange of this filing information will eliminate the Court Clerk's data entry responsibility, and continued progress and improvement can be measured by tracking the number of data errors reported for correction for current exchanges.

Redundant data entry is an example of a measure that it is important to collect against a baseline that is based on a non-real-time exchange; the initial difference between the costs and time associated with a paper or FTP-based exchange compared to a real-time exchange will likely be significant and an immediately demonstrable measure of improved justice process as a result of automation.

6.3.3.2 Reduce Delays in the Flow of Information Between Agencies

Because the current justice system mostly relies on the manual transfer of documents between agencies, the flow of information is not as reliable and predictable as it could be. Even with the current electronic exchanges, most are based on batch transactions and therefore do not occur in real-time.

There are two ways in which more timely information flow can be measured: One way is by reducing the delays between events in the criminal justice process. Examples of these measures include:

- Reducing the number of continuances per case originating from scheduling conflicts
- Increasing the number of hearings held as scheduled
- Reducing the average days from arrest to arraignment or arrest to disposition.[53]

A second way is measuring the timeliness of information that passes through the system. Examples of these measures include:

- Improved turnaround time for positive identification of arrested persons
- Availability of all orders issued by the court by close of court day
- Ability of all public safety agencies to determine the status of an individual, case, or charge within a designated amount of time (minutes) with a status currency of 24 hours
- Ability of all public safety agencies to access an individual's record within a designated amount of time (minutes) with a status currency of 24 hours
- All public safety agencies shall be able to determine pre-adjudication information within 24 hours
- Ability to determine non-criminal case information within 24 hours
- Change in the of hours it takes to respond to request from public
- Change in the number of minutes it takes to complete criminal history background check
- Change in the average number of days from arrest to arraignment

6.3.3.3 Improved Staff Productivity

Improving staff productivity is a valuable goal and one that appears to be extremely important to many criminal justice agencies in Iowa. While electronic sharing of information should intuitively reduce staff burdens and increase productivity, the MAXIMUS/URL survey identified significant concern among law enforcement and Court practitioners about the staffing implications of justice information sharing.

By eliminating redundant data entry and reducing mistakes that need correcting, integration will greatly increase staff productivity. Data will only need to be entered once

[53] *SEARCH Presentation.*

into the criminal justice system and propagation of the data to receiving agencies and databases will be electronic. Integration should also reduce the number of telephone calls, manual delivery of documents, and manual document generation – all which take staff time and effort. The staff will be able to focus on more strategic goals within the State.

Examples of measures associated with improved staff productivity include:

- Increase in the number of current exchanges transmitted daily
- Improve time of processing of judgment document originating from judge, pass through hands of clerk of court and then to DOC
- Mean time to complete a criminal history check using systematic state audit
- Decrease in amount of time it takes to enter a warrant into state warrant repository
- Decrease in amount of time it takes to enter a protective order into state repository
- Decrease in number of hours it takes to a respond to request from the public
- Decrease in number of minutes it takes to complete criminal history background check
- Decrease in the average days from arrest to arraignment

6.3.3.4 Reduced Paper Costs

While there is no known measure of current paper costs, electronic transfer of documents between agencies should greatly reduce the need for paper documents and multiple copies of documents sent between agencies. The system will have the ability to electronically transfer not only the data in a document, but the document format so that it appears at the receiving agencies in the same format it was sent. Digital signatures could allow for the documents to be authorized online.

Examples of ways to measure the reduced paper costs include:

- Decrease in costs of copy paper
- Decrease in costs of storing paper
- Decrease in costs of buying paper
- Decrease in costs associated with producing forms

6.3.3.5 Reduced Dependence on Individuals with Other Stakeholder Organizations

The current justice system is “people-dependant” in terms of relying on certain individuals or roles (such as the Court Clerk) for the transfer of information and documents between agencies. In many cases, information exchange is verbal with no written record of the exchange. This becomes unreliable and untraceable in many cases.

With integration, exchange processes between agencies will be secure, traceable, and documented. The agencies can be guaranteed that they are receiving reliable data in a timely manner without having to rely on any particular individual.

Examples of these measures include:

- Change in the number of phone calls among criminal justice entities
- Change in the number of hours spent searching other automated systems
- Change in the number of hours spent filing paper manually
- Change in the number of hours spent by staff looking for hard copy files
- Reduce the costs of copying paper for other governmental entities

6.3.3.6 Reduce Time Locating Information or Data

Currently, criminal justice practitioners must spend time locating information and checking for updates with other agencies. With integration, data should be available online to the appropriate users in real-time and reduce the need to telephone or otherwise ask justice personnel or clerks for timely information which may affect criminal charges or otherwise. The data should be easily accessible and reliable.

Many of the measures listed in Section 6.3.3.5 above are applicable here as well.

6.4 Implementing Performance Measurement in Iowa

Creating a performance measurement system for the CJIS effort in Iowa is a critical undertaking and will require significant thought, planning, and effort. The dividends this effort can pay could be exceptional, however: if the CJIS Program Office and Advisory Committee can begin quantifying the benefits of integrated justice early on and map it to cost savings or improvements in public safety and the quality of life, the likelihood of acquiring and maintaining funding from the legislature and other funding sources will increase.

In other words, establishing performance measures and including this information in the yearly tactical/operational plan will help demonstrate to policymakers the benefit criminal justice integration is having on the community and may well justify the expense associated with its continued implementation.

The following are some suggestions that the MAXIMUS/URL Team has for the CJIS Program Office with regard to establishing and maintaining performance measures for CJIS in Iowa:

Create a Baseline on Select Indicators. As mentioned above, creating a baseline of selected indicators based on the current paper-based and/or FTP exchanges will allow the CJIS Program Office to easily determine the benefits (increased personnel efficiency,

increased availability of information to the justice enterprise, etc.) once an exchange happens real-time as a part of data flow. This baseline will be important initially in justifying the need for CJIS and building support for funding implementation.

Implement Performance Measures in Phases. Developing the measures and formulas behind them are typically best done as part of a group process, to ensure that all parties agree that the measure, data, and formula are legitimate. Pick a few key indicators each year to develop and pilot. After piloting the measures, proactively elicit feedback and make necessary modifications to ensure the validity of the measure moving into the future.

Creating Measures Takes Time. Similarly, be aware that the creation of good performance measures takes time. There are many pitfalls to establishing sound measures: they can be too complex, generalized from limited data, or contain spurious relationships.

Identify Best Practices. While the implementation of CJIS performance measures is a relatively new concept, more and more agencies are interested in being able to quantify the effects of the integration effort. As a result, there is a growing body of literature about performance measures, including the sources used for this section of the plan. Review those sources and any other available information when planning for the implementation of phased CJIS performance measures in Iowa.

Tie Performance to Yearly Tactical Budgets and Legislative Requests. Lastly (but perhaps most importantly), performance-based information should be included in CJIS Program Office yearly budgets, requests to the legislature, and annual reports. Well-planned and collected information will invariably demonstrate the power and benefit of integration.

7 Appendix A: Local Implementation Costs

Establishment of the Iowa CJIS Broker will not necessarily facilitate the automated sharing of information between the entities of the Iowa criminal justice practitioner community. Local county and municipalities, as identified in the As-Is Assessment, may have two significant barriers to participation in the envisioned Iowa CJIS solution:

1. Lack of a management system that provides automated support of the business practices in the local agency (e.g., RMS, JMS, CMS, etc.)
2. Lack of the appropriate network connectivity to transport exchanges between sharing partners.

These barriers are not directly within the scope of the Iowa CJIS Strategic Plan, however if they are not addressed they could create a considerable gap in the amount of information available to the Iowa criminal justice community and minimize the impact of its deployment to achieving the objectives of the Plan. Each agency has its own responsibility for implementation of the applications necessary to support their day-to-day business operation, and the plan does not account for the ongoing cost of ownership of the solutions already deployed in Iowa as they are also not within the scope of the CJIS initiative. Like their state counterparts, local agencies will also need to make business cases to receive funding from their own governmental budget processes to overcome these barriers. The information presented here is intended to have the following outcomes:

- Acknowledgement that the deployment of the CJIS Broker is not going to solve disparate automation and connectivity barriers at the local level
- Recognition that the responsibility for addressing those issues is at the local agency level
- Provides a benchmark that could be used by local agency to initiate activities to secure automated management solutions and plan for their own cost of ownership

Both examples illustrate the costs that would be incurred for setting up a five-person office with the identified hardware and software components. Additional costs can be estimated by increasing the number of users and re-calculating the estimated impact.

7.1 One-Time Costs

One-time costs include the following components that would be necessary to deploy a management system with appropriate hardware, software, and network connectivity. In these examples the term Management System could be used to indicate a Record Management System, Jail Management System, or a Case Management System. The configuration consists of following elements:

- PC – A personal computer necessary to run the client user interface of the system.
- Business Server – The physical server that would host the business application logic software components of the case management system.
- Database Server – The physical server that would host the persistent storage of case management records for the management system.
- Management Server Software – The application software used to support the business processes and policies of the management system .
- Management Client Software – The client software that supplies the user interface for the management system. In the low-end solution, this cost is expected be covered in the Management Server Software cost.
- RDBMS Software – RDMBS software license necessary for persistent storage.
- Software Training – User, administrative, and other necessary training to properly utilize the management system selected.
- Network Infrastructure – One-time set up fees for the necessary network connection to support CJIS.

The following table summarizes the one-time costs that could be expected from the implementation of the management system as described.

One-Time Costs	Low-End Option			High-End Option		
Description	**Units Required**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
PC	5	$1,048.00	$5,240.00	5	$2,266.00	$11,330.00
Business Server	1	$9,098.72	$9,098.72	2	$19,995.00	$39,990.00
Database Server	1	$33,027.39	$33,027.39	2	$56,938.95	$113,877.90
Management Server Software	5	$580.00	$2,900.00	1	$335,199.00	$335,199.00
Management Client Software	0	$0.00	$0.00	5	$2,867.00	$14,335.00
RDBMS Software	2	$790.00	$1,580.00	4	$8,800.00	$35,200.00
Software Training	4	$1,200.00	$4,800.00	4	$3,600.00	$14,400.00
Network Infrastructure	1	$2,714.00	$2,714.00	1	$3,643.00	$3,643.00
Total			**$59,360.11**			**$567,974.90**

7.2 Recurring Costs

The following table summarizes the recurring annual costs that could be expected from the implementation of the management system as described.

Recurring Costs	Low-End Option			High-End Option		
Description	**Charge**	**Unit Cost**	**Total**	**Units Required**	**Unit Cost**	**Total**
Hardware Maintenance	18%	$34,075.39	$6,133.57	18%	$59,204.95	$10,656.89
Software Maintenance	19%	$580.00	$110.20	19%	$335,199.00	$63,687.81
Annual Network Connectivity	1	$27,252.00	$27,252.00	1	$43,479.00	$43,479.00
Total			**$33,495.77**			**$117,823.70**

8 Appendix B: Business Survey Questions

Law Enforcement agencies use Affidavit and Complaint forms that differ from agency to agency. Is it likely that these forms could be standardized across the State? (1 = Not Likely, 5 = Very Likely)

The Complaint and Trial Information forms do not contain identifying numbers, such as the Document Tracking Number (DTN), a DCI#, FBI#, or Social Security Number. The "Greensheet" is used to pass this information between agencies for the purpose of maintaining a complete criminal history. However the Greensheet does not improve the agency's identification of a person or case information in their workflow. If the offender has been booked would it be difficult to include these identifiers on the forms? (1 = Very Difficult, 5 = Not at All Difficult)

The Uniform Traffic Citation is electronically sent from Law Enforcement to the Courts, avoiding reentry of the ticket. Non-traffic Citation and Complaints are paper-based and sent to the Court manually for reentry. For Citations and Complaints to be sent electronically, it would require Law Enforcement to enter the Citation and Complaint into the RMS system in a timely manner. Do you see this as likely to occur in your jurisdiction? (1 = Very Unlikely, 5 = Very Likely)

In more populated jurisdictions, the County Attorney may review all Complaints on indictable offenses before they are filed with the Court. In less populated jurisdictions, the Law Enforcement may directly file directly with the Court. Other business practices also vary by jurisdiction size. Staff resources and the number of filings in the jurisdiction impact these differences.

Please check the appropriate answer below:
The staff resources in the jurisdiction will not allow for standardized practices.

Using the same example as above, would direct filing with the Court impact the agency's ability to file charges as they think best?

Again, using the same scenario as above, in your opinion, do the benefits derived from standardized automation outweighs the jurisdiction-level business process impacts?

Many forms, including Court Orders, vary among agencies in what information they contain, what they are called, and how they are organized. This has allowed for the customization of the forms (orders) to meet the requirements of the agencies (judges, clerks, County Attorneys, etc.). If the forms could be standardized in such a way that these agency requirements are met, it is likely more specific information would need to be collected as much of this is currently buried in text.

Please check the box that best represents your views on the following statement: Customized forms are necessary to practice my role in justice.

Using the same example as above, please assess the following statement: Standardized forms and information would be an intrusion.

If the goal of exchanging information with other criminal justice agencies is to reduce duplicate entry and improve the quality of the information, the data now on forms would need to be entered into the sending and receiving agencies' systems. This may require the entry of additional information as well as timely data entry. Another benefit could be avoiding the need to fill out the forms by hand, similar to how TraCS works. Do you see the timely data entry as barrier to your current business process?

Referencing the question above, what are your ideas about how to improve data integrity in support of information sharing?

Warrants are issued by the Court and given to either Law Enforcement or the Sheriff. Law Enforcement and the Sheriff then enter the warrant into the IOWA System and in some cases a local warrant database. With a number of warrants, additional information is entered into the IOWA System to meet Law Enforcement requirements. Once a warrant is in the IOWA System, it could become out of sync with the Court, particularly when the offender has been located but a decision was made not to transport the offender. The automation of warrant exchanges would greatly reduce the amount of data entry, particularly for Sheriffs. It would also improve the synchronization between the key systems. Please respond to the questions below addressing the feasibility of automating this process.

If perpetrator and victim information was accessible, such as when the perpetrator would be released, would your agency use this information?
How would you handle the confidentiality of this information?

Information regarding the status of County Prosecutor Diversion and Juvenile Informal Adjustments, as examples, are not available to the justice system at large.

Many orders, notifications, or other types of information are shared verbally. Would it be worth the effort to enter these orders into your system and or have the systems automatically notify interested parties such as Law Enforcement and Community Corrections? (1 = Very Much, 5 = Not Much)

Interested parties would benefit from notification around release from jail. This might mean more entry for the Jails and possibly the Courts. Is this worth the business change? (1 = Very Much, 5 = Not Much)

If the automated information sharing between your agency and others in the criminal justice system required business practice changes, more timely data entry, or changes in

forms, do you see these as worthwhile changes despite the effort? (1 = Very Much, 5 = Not Much)

Security is a significant part of information sharing; do you believe trusting another agency with your data is safe?

What, in your opinion, would allow for the electronic sharing of data to be secure?

Is your agency able or willing to adopt the security requirements of another agency to exchange information electronically?

Is sharing common case management, record management, jail management systems with other agencies OR adopting standards with existing systems a manageable direction for your agency?

If you have any additional information or opinions about the CJIS initiative or your IT investment, we would appreciate hearing them.

9 Appendix C: Glossary

Application Server - A middle tier component that is dedicated to acting as a container for application business logic, programs, content, and possibly authentication. This is vendor-supplied software that provides an environment to host application programs. Common application environments are J2EE and .NET.

Broker - A messaging system for applications that includes a message transport, rules engine, and formatting engine. Specifically, a broker is software that provides an interface between applications, allowing them to send data back and forth to each other asynchronously. Data sent by one program can be stored in a queue and then forwarded to the receiving program when it becomes available to process it. Without using a common message transport and queuing system such as this, each application must be responsible for ensuring that the data sent is received properly. Maintaining communications between different types of applications as they are revised and eventually replaced with newer architectures creates an enormous programming burden in the large enterprise.

CJIS - Criminal Justice Information System - Refers to the ability to share critical information electronically at key decision points throughout the justice enterprise.

COTS - commercial off-the-shelf software - Refers to ready-made merchandise that is available for sale.

Dual-mode Authentication - Also known as two-factor authentication, this authentication method incorporates the use of a device that generates a unique identification number meaningful only when paired with a PIN known only to the owner of the device. That PIN/identification number combination is necessary to allow the user to log in to the network/service.

Firewall - The primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise.

In the organization, a firewall can be a stand-alone machine or software in a router or server. It can be as simple as a single router that filters out unwanted packets, or it may comprise a combination of routers and servers each performing some type of firewall processing.

FTP - File Transfer Protocol - A protocol used to transfer files over a TCP/IP network.

GJXDM -Global Justice XML Data Model (GJXDM) - An object-oriented data model for organizing the content of a data dictionary (the Global JXDD) in a database. The purpose of the Global JXDM is to provide a consistent, extensible, maintainable XML schema reference specification for data elements and types that represent the data requirements of the general justice and public safety communities.

IEP - An Information Exchange Package - represents a set of data that is transmitted for a specific business purpose. It is the actual XML instance that delivers the payload or information.

IEPD - Information Exchange Package Documentation - A collection of artifacts that describe the structure and content of an Information Exchange Package. It does not specify other interface layers (such as web services).

J2EE - Java 2 Platform, Enterprise Edition - A platform from Sun for building distributed enterprise applications. J2EE services are performed in the middle tier between the user's machine and the enterprise's databases and legacy information systems.

Middle Tier - Conceptual level term to identify the architecture layer residing between the database tier and the end-user tier that contains the application logic, content, and possibly authentication schemes.

.NET - Microsoft's framework for Web services and component software; corollary to Sun's J2EE.

RDBMS - Relational Database Management System – Any of a number of database systems that employ a relational architecture to data structures as opposed to other models such as hierarchical.

SAN - Storage Area Network - A network of storage disks, usually centralized, that are used to off-load storage from local server drives to high-speed, redundant storage architectures.

SFTP - Secure File Transfer Protocol – A secured (encrypted) version of FTP.

SMTP - Simple Mail Transfer Protocol - The standard e-mail protocol on the Internet and part of the TCP/IP protocol suite. SMTP defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

SOAP - Simple Object Access Protocol - A message-based protocol based on XML for accessing services on the Web. Initiated by Microsoft, IBM and others, it employs XML syntax to send text commands across the Internet using HTTP.

Service-Oriented Architecture (SOA) - An application architecture in which all functions, or services, are defined using a description language and have interfaces that are called to perform business processes. Each interaction is independent of each and every other interaction and the interconnect protocols of the communicating devices (i.e., the infrastructure components that determine the communication system do not affect the interfaces).

Software Development Life-Cycle -Refers to the phases an information system must go through from the time it is conceived and the time it is available for use. Specific steps include: 1) requirements analysis; 2) design; 3) development; 4) testing; 5) production; 6) maintenance; 7) enhancement and evolution.

Transaction Processing Analysis - An analysis of each participating system's business processes to arrive at a Use Case of how and at what point in the process the tasks are accomplished. The goal of this effort is to identify specific points within the workflow where data exchanges are initiated or where a data exchange is received, initiating a process within the workflow. This bidirectional analysis is key in determining the trigger events within the system that not only send a transaction but also what system processes are initiated by the receipt of a transaction.

TCP - Transmission Control Protocol - The transport protocol within the TCP/IP protocol suite. TCP ensures that all data arrive accurately and 100% intact at the other end.

User Interface (UI) - The combination of menus, screen design, keyboard commands, command language and online help, which creates the way a user interacts with a computer. If input devices other than a keyboard and mouse are required, this is also included. In the future, natural language recognition and voice recognition will become standard components of the user interface.

VPN - Virtual Private Network - A private network that is configured within a public network (a carrier's network or the Internet) that is usually, but not always encrypted.

Web Service - Web-based applications that dynamically interact with other Web applications using open standards that include XML, UDDI, and SOAP. Such applications typically run behind the scenes as one program "talking to" another (server to server).

XML - eXtensible Markup Language - An open standard for describing data from the World Wide Web Consortium (W3C). It is used for defining data elements on a Web page and business-to-business documents. XML uses a similar tag structure as HTML; however, whereas HTML defines how elements are displayed, XML defines what those elements contain. While HTML uses predefined tags, XML allows tags to be defined by the developer of the page. Thus, virtually any data items, such as "product," "sales rep," and "amount due," can be identified, allowing Web pages to function like database

records. By providing a common method for identifying data, XML supports business-to-business transactions and has become "the" format for electronic data interchange and web services.

XML Accelerator - A component that off-loads XML processing from the application logic to a dedicated hardware device, improving overall performance.

Source:
TechWeb at http://www.techweb.com/